Device Independent Quantum Key Distribution with a Single Measurement per Site

Raffaele D'Avino,[1] Lorenzo Caramelli,[1] Raja Yehia,[1] Gabriel Senno,[1,2]
Roberto González Pousa,[1] Antonio Acín,[1] and Tamás Kriváchy[1]

[1] *ICFO - Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain*
[2] *Quside Technologies S.L., C/Esteve Terradas 1, 08860 Castelldefels, Barcelona, Spain*

I. INTRODUCTION

Device-independent quantum key distribution (DIQKD) is the gold standard for cryptographic security [1, 2]. Such protocols are based on the two interested parties, Alice and Bob, performing a Bell-test. Achieving a high enough score proves that their outcomes are highly correlated and not influenced by external sources, allowing for the establishment of a private shared key.

It is well-known that in order to execute a successful DIQKD protocol, Alice and Bob must both use non-commuting measurements, as this is necessary to violate a Bell inequality. Since the choice of measurements of a given round should not be known to or influenced by an adversary, these are typically extracted from some source of randomness on the spot – one randomness source in Alice's lab and one in Bob's.

In recent years, the foundational concept behind DIQKD, Bell nonlocality, has been extended to networks with multiple parties and multiple independent sources [3–6]. One fascinating aspect of these generalizations is that in certain cases, nonlocal phenomena exist even without non-commuting measurements. A seminal example is the RBG4 distribution introduced in [7], which demonstrates genuine network nonlocality in a ring network, where neighboring parties are distributed quantum states from bipartite sources. Each party performs the same fixed measurement in every round, and the resulting correlations cannot be reproduced by any classical model consistent with the network structure, making local randomness for measurement choices unnecessary. Several experimental proposals [8–10] and implementations exist for the phenomenon [11, 12].

Crucial to these claims of nonlocality is the assumptions that local hidden variables that would explain the correlations mimic the network structure, maintaining independence among these themselves. Indeed, under such assumptions, not only can one show nonlocality, but also certify randomness of the outcomes in a fully device-independent [13] manner. Whereas one may be able to make arguments for the independence of sources in well-controlled environments, in large networks this assumption may be quite far-fetched, where a user can not control or check each part of the network. In [14] the authors show that this is in fact not necessary, as claims of nonlocality and randomness are robust against the topology of the network. Specifically, as long as a small, 3-party region of the network satisfies the independence assumption, nonlocality can be proven, as well as device-independent randomness on the outcome of the central of the 3 parties.

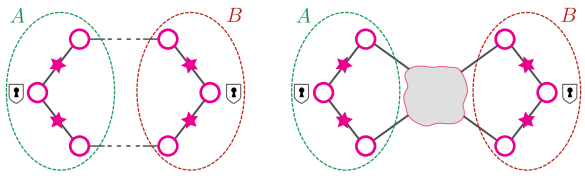

FIG. 1. (a) In order to implement the proposed no-input DIQKD protocol, the users request the distribution of entangled states from sources (stars) in a ring network, which are measured at nodes (circles) using entangling measurements, establishing correlations between Alice's (green) and Bob's (red) labs. The outcomes of the central nodes in the labs can be distilled to a secret key, given that the nodes in-between announce their outcomes. (b) In the security proof Alice and Bob do not assume anything about the structure of the network in-between them, i.e. the rest of the network outside their labs could be collaborating (grey cloud), moreover they do not trust the workings of the independent devices within their own labs either.

Here, we propose a DIQKD protocol where all parties in the network perform the same measurement in each round. Building on the topological robustness results, we require the independence of sources assumptions to only be satisfied within the local neighborhoods of Alice and Bob, in their "labs" (Fig. 1). This is analogous to the independence of the local randomness sources used in conventional DIQKD, where input randomness is necessary, and should be uncorrelated from anything outside the lab. We prove security against collective attacks, and assess how security against general attacks could be proven if the i.i.d. assumption is dropped for the central part of the network.

Besides being a conceptually novel form of DIQKD, requiring no measurement settings, our work closes the loop on network nonlocality. In particular, whereas network nonlocality studies multiple parties and sources, we show how this can be meaningfully turned into a bipartite setup (see Fig. 1. We end up with a scenario which is directly comparable to the standard Bell setup, in that it is phrased for two parties, has certified randomness in the outcomes, and that those outcomes can be used for device independent protocols. Moreover, for our proto-

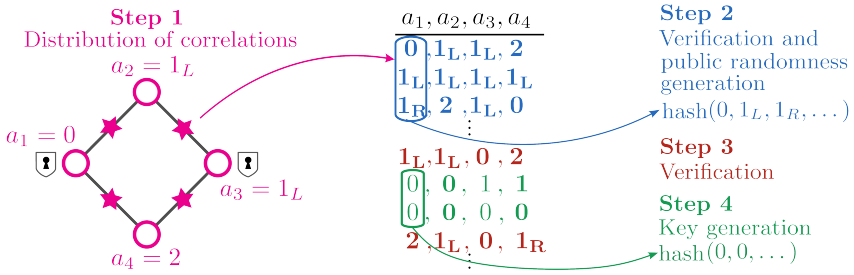

FIG. 2. Overview of the protocol for 4 parties, where A_1 and A_3 wish to establish a secret key. **Left:** Step 1 (in magenta): The four parties, arranged in a ring network, perform RGB4 measurements on the states they receive, producing coarse-grained outcomes $\{a_k\}_{k=1}^4$. The two parties who will share the final key are indicated with a key symbol. **Middle:** Example outcomes for each party, with publicly announced results in **bold**. **Right:** Step 2 (in blue): Some outcomes are publicly announced to verify RGB4 correlations. A_1's outcomes, after applying a hash H, generate public randomness to determine later rounds as verification or key generation. Step 3 (in red): Verification rounds where all outcomes are revealed to check the RGB4 correlations. Step 4 (in green): Key generation rounds where A_1 and A_3 derive a shared secret key from A_2 and A_4, with hash H applied to the resulting string.

col, since there are no distinguished parties within the network in the correlation establishment phase, it can be used to build up and store correlations classically, which at a later time can be used to create a secret key between any two parties in the network. We believe the conceptual shift in this work will help push towards potential applications built on the foundational concept of nonlocality without inputs.

II. PROTOCOL SUMMARY

The protocol is based on distributing maximally entangled states $(|01\rangle + |10\rangle)/\sqrt{2}$, and conducting the RGB4 measurement [7] at each node in a ring network,

$$\Big\{ |00\rangle\,,\ u\,|01\rangle + v\,|10\rangle\,,\\ v\,|01\rangle - u\,|10\rangle\,,\ |11\rangle \ \Big|\ u^2+v^2=1,\ u,v\in\mathbb{R}\Big\}, \tag{1}$$

with outcomes labeled as $\{0, 1_L, 1_R, 2\}$. The nonlocality, and device-independent randomness of the resulting distribution can be proven from so-called token counting properties [7, 15]. Specifically, each source can be seen as distributing a single token (excitation) in a superposition, and the measurement can be seen as a counting of the number of incoming tokens, plus outputting some additional coherence information (whether the outcome was 1_L or 1_R). In [13] and later generalized in [14], it is shown that correlations arising from this class of distributions admit self-testing, allowing the underlying quantum realization to be partially certified solely from the observed statistics. As a result, the outcome of any party is nondeterministic from the perspective of an eavesdropper.

Our protocol relies on a parity coarse-graining of the outcomes, $0, 2 \mapsto 0$ and $1_L, 1_R \mapsto 1$, yielding a binary variable. The parity of the total network's outcomes is known to all participants, as this is determined by the number of sources used. The key point of the protocol is that everyone except Alice and Bob announce their parity. In order to infer the parity of Alice, one must know the parity of Bob, and vice-versa. E.g. if the total parity is even, and the summed announced parities are even, then Alice and Bob's summed parity must also be even, leaving two options: $a = 0, b = 0$ or $a = 1, b = 1$. This allows the two parties to establish a secret key, while no-one on the outside can. The certification of randomness of the parties is derived by extending the techniques of Ref. [14]. See Fig. 2 for a 4-party example.

In order to ensure themselves that the protocol is secure, not all rounds can be used for key generation. In some rounds Alice and Bob must also announce their outcomes. In these rounds, they can verify that the RGB4 distribution is being generated over the network. This in turn, certifies that their outcomes contain randomness, as given by a min entropy bound. The protocol works as follows: first, the network conducts n rounds of the RGB4 strategy. Then, the first portion of these are used for verification, where all parties announce their full outcomes. If sufficiently close to the RGB4 distribution, then the outputs of these first rounds are certified to be random and are used to select which of the subsequent rounds will be used as key generation rounds, and which will be used as further verification rounds. The random choice of verification rounds ensures that key generation rounds are not tampered with.

Security of the protocol is shown under the following assumptions: the independence of sources assumptions hold within the labs of A and B (as shown in Fig. 1b), attackers conduct collective (iid) attacks, using finite-dimensional quantum systems (a technicality of the proof), and that there are asymptotically many rounds.

III. DISCUSSION AND OPEN QUESTIONS

It is instructive to compare our network-based framework with the standard Bell-nonlocality setting (see

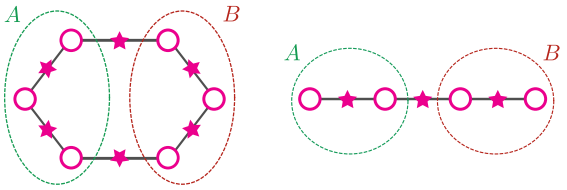

FIG. 3. Comparison between our network (left) and the four-party line network (right) known to be equivalent to the standard Bell scenario [5]. In each case, the nodes corresponding to the effective "Alice" and "Bob" are highlighted.

Fig. 3). In a Bell test, one studies behaviours $\{p(ab|xy)\}_{a,b,x,y}$, where the inputs x and y must be chosen freely—namely, independently of any shared past or adversarial system—to avoid locality and measurement-independence loopholes. From a network perspective, however, these "free" inputs can themselves be generated by additional parties in a larger correlation scenario. Indeed, as shown in [5], the usual Bell scenario is equivalent to a four-party line-network in which the inputs arise as outcomes of the two outer nodes. Under this equivalence, the standard Bell assumptions (including measurement independence) translate directly into an *independent-sources* assumption in the network. This observation clarifies that the independence requirement on the sources within the labs in our framework is not a stronger assumption than those made in Bell experiments; rather, it is the natural network-theoretic analogue of the measurement-independence condition that underlies all device-independent protocols.

The analysis in Ref. [16] pinpoints an issue that is crucial in networks with no inputs - namely that the i.i.d. assumption can not be left away without introducing a memory loophole in no-input scenarios such as ours. Given the equivalence of standard Bell nonlocality to a no-input line network scenario (Fig. 3b), one may ask why the memory loophole does not appear there. In non-iid DIQKD security proofs one assumes a lower bound on the quality of the input randomness, implying that it cannot completely be controlled or pre-programmed by an adversary. Typically, one assumes an iid property for the input randomness, with only recent attempts to relax this [17, 18]. In any network setup where the inputs are externalized, as shown in Fig. 3b for the standard Bell scenario, the iid assumption can only completely be left away for one of the sources, otherwise the memory loophole of Ref. [16] is a risk. In our setup a natural choice is to keep the iid assumption on Alice and Bob's immediate neighborhood, which one can imagine as their laboratories, leaving the rest of the network, the untrusted center, to be non-iid. It is yet unclear how well the iid assumption on the labs can be relaxed, analogously to [17, 18]. Presumably the most straight-forward way would be to generalize the results of [13, 14] by giving a robust bound for the min entropy, even under noisy realizations of the ideal distribution. Then the generalized entropy accumulation theorem may be applicable, similarly as in [19]. Note that such a generalization would also eliminate the need for the asymptotic limit assumption. Thus this would be crucial piece to make the proposed protocol practical, and is left for future work.

Furthermore, note that any randomness that we use as input in our protocol, namely for authentication, can be generated before starting the protocol. Indeed, even in standard DIQKD, the parties must come together physically in order to establish a shared random seed that they use for authentication. This is the case also for us; and when they come together in an isolated lab, they can run only the verification part of our protocol (or equivalently, the randomness certification in Ref. [13]) to obtain the random seed with no inputs used. This allows our no input (fixed measurement setting) protocol to be a protocol which requires no input randomness at all. Note however, that this technique could also render standard DIQKD to be operated without any randomness as an input. For both cases, once authentication kick-starts the protocol, the freshly generated secret key can be used to further authenticate and do privacy amplification.

Finally, note that our proposal gives an interesting opportunity for DIQKD in larger network with multiple labs. In such a scenario the correlations can be established beforehand, each party conducting the same measurement for large number of rounds. Once the *classical outcomes* are stored, one can wait indefinitely before deciding which parties in the network share a secret key. This allows one to mitigate the use of quantum memories for overcoming bottlenecks in quantum channel capacities in the network, and opens the path to pre-establishing a DIQKD resource among network participants. This can be particularly relevant for applications in decentralized networks where for long periods of time key exchange is not needed, e.g. overnight, during which correlations are built up, and then suddenly a large bandwidth is needed, and it is unknown beforehand between which parties in the network the bandwidth will be needed. At this point the pre-established raw outcomes can be used.

IV. CONCLUSION

In summary, we have introduced a protocol for quantum key distribution and conference key agreement in network scenarios that does not rely on local input randomness, departing conceptually from the standard view that multiple different measurements are necessary for quantum cryptography. By performing pre-decided measurements at each node and exploiting the structure of the network, we showed that it is possible to establish secret keys even when most nodes and sources are untrusted. This approach preserves the essential device-independent features of Bell inequality-based protocols while introducing a natural network-theoretic perspective on assumptions such as source independence.

[1] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, *et al.*, Advances in quantum cryptography, Advances in optics and photonics **12**, 1012 (2020).

[2] V. Zapatero, T. van Leent, R. Arnon-Friedman, W.-Z. Liu, Q. Zhang, H. Weinfurter, and M. Curty, Advances in device-independent quantum key distribution, npj quantum information **9**, 10 (2023).

[3] C. Branciard, N. Gisin, and S. Pironio, Characterizing the nonlocal correlations created via entanglement swapping, Phys. Rev. Lett. **104**, 170401 (2010).

[4] C. Branciard, D. Rosset, N. Gisin, and S. Pironio, Bilocal versus nonbilocal correlations in entanglement-swapping experiments, Phys. Rev. A **85**, 032119 (2012).

[5] T. Fritz, Beyond bell's theorem: correlation scenarios, New Journal of Physics **14**, 103001 (2012).

[6] A. Tavakoli, A. Pozas-Kerstjens, M.-X. Luo, and M.-O. Renou, enBell nonlocality in networks, Reports on Progress in Physics **85**, 056001 (2022).

[7] M.-O. Renou, E. Bäumer, S. Boreiri, N. Brunner, N. Gisin, and S. Beigi, Genuine quantum nonlocality in the triangle network, Physical review letters **123**, 140401 (2019).

[8] P. Abiuso, T. Kriváchy, E.-C. Boghiu, M.-O. Renou, A. Pozas-Kerstjens, and A. Acín, Single-photon nonlocality in quantum networks, Phys. Rev. Res. **4**, L012041 (2022).

[9] T. Kriváchy and M. Kerschbaumer, Closing the detection loophole in the triangle network with high-dimensional photonic states, Phys. Rev. Lett. **135**, 160803 (2025).

[10] O. Meskine, I. Šupić, D. Markham, F. Appas, F. Boitier, M. Morassi, A. Lemaître, M. Amanti, F. Baboux, E. Diamanti, and S. Ducci, Experimental fiber-based quantum triangle-network nonlocality with a telecom AlGaAs multiplexed entangled-photon source, PRX Quantum **6**, 020313 (2025).

[11] N.-N. Wang, C. Zhang, H. Cao, K. Xu, B.-H. Liu, Y.-F. Huang, C.-F. Li, G.-C. Guo, N. Gisin, T. Kriváchy, and M.-O. Renou, Experimental genuine quantum nonlocality in the triangle network (2024), arXiv:2401.15428 [quant-ph].

[12] E. Polino, D. Poderini, G. Rodari, I. Agresti, A. Suprano, G. Carvacho, E. Wolfe, A. Canabarro, G. Moreno, G. Milani, *et al.*, Experimental nonclassicality in a causal network without assuming freedom of choice, Nature Communications **14**, 909 (2023).

[13] P. Sekatski, S. Boreiri, and N. Brunner, Partial self-testing and randomness certification in the triangle network, Phys. Rev. Lett. **131**, 100201 (2023).

[14] S. Boreiri, T. Kriváchy, P. Sekatski, A. Girardin, and N. Brunner, Topologically robust quantum network nonlocality, Physical Review Letters **134**, 010202 (2025).

[15] M.-O. Renou and S. Beigi, Network nonlocality via rigidity of token counting and color matching, Physical Review A **105**, 022408 (2022).

[16] M. Weilenmann, C. Budroni, and M. Navascues, Memory attacks in network nonlocality and self-testing, Quantum **9**, 1735 (2025).

[17] M. Kessler and R. Arnon-Friedman, Device-independent randomness amplification and privatization, IEEE Journal on Selected Areas in Information Theory **1**, 568 (2020).

[18] M. Sandfuchs, C. Ferradini, and R. Renner, Randomness from causally independent processes (2025), arXiv:2510.05203 [quant-ph].

[19] T. Metger and R. Renner, Security of quantum key distribution from generalised entropy accumulation, Nature Communications **14**, 5272 (2023).

Device Independent Quantum Key Distribution with a Single Measurement per Site

Raffaele D'Avino,[1] Lorenzo Caramelli,[1] Raja Yehia,[1] Gabriel Senno,[1,2]
Roberto González Pousa,[1] Antonio Acín,[1] and Tamás Kriváchy[1]

[1] *ICFO - Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain*
[2] *Quside Technologies S.L., C/Esteve Terradas 1, 08860 Castelldefels, Barcelona, Spain*

(Dated: Feb. 2026)

Device-independent quantum key distribution (DIQKD) guarantees cryptographic security based solely on the violation of Bell inequalities, where each party chooses measurements randomly in each round. Recent extensions of Bell nonlocality to networks with multiple parties and independent sources have revealed scenarios in which nonlocal correlations, and the associated certified randomness, can be achieved even when all parties perform the same measurement in every round, eliminating the need for local measurement randomness. Building on these insights, this work proposes a DIQKD protocol in which Alice and Bob perform fixed, identical measurements in each round. Security relies on independence assumptions for certain devices, analogous to those used in network nonlocality and to the standard independence of local randomness sources in conventional DIQKD.

I. INTRODUCTION

Device-independent quantum key distribution (DIQKD) is the gold standard for cryptographic security [1, 2]. Such protocols are based on the two interested parties, Alice and Bob, performing a Bell-test. Achieving a high enough score proves that their outcomes are highly correlated and not influenced by external sources, allowing for the establishment of a private shared key.

It is well-known that in order to execute a successful DIQKD protocol, Alice and Bob must both use non-commuting measurements, as this is necessary to violate a Bell inequality. Since the choice of measurements of a given round should not be known to or influenced by an adversary, these are typically extracted from some source of randomness on the spot – one randomness source in Alice's lab and one in Bob's.

In recent years, the foundational concept behind DIQKD, Bell nonlocality, has been extended to networks with multiple parties and multiple independent sources [3–6]. One fascinating aspect of these generalizations is that in certain cases, nonlocal phenomena exist even without non-commuting measurements. A seminal example is the RBG4 distribution introduced in [7], which demonstrates genuine network nonlocality in the triangle network. Each party performs the same fixed measurement in every round, and the resulting correlations cannot be reproduced by any classical model consistent with the network structure, making local randomness for measurement choices unnecessary. Several experimental proposals [8–10] and implementations exist for the phenomenon [11, 12].

Crucial to these claims of nonlocality is the assumptions that local hidden variables that would explain the correlations mimic the network structure, maintaining independence among these themselves. Indeed, under such assumptions, not only can one show nonlocality, but also certify randomness of the outcomes in a partially device-independent (steering) [13] or fully device-independent [14] manner. Whereas one may be able to make arguments for the independence of sources in well-controlled environments, in large networks this assumption may be quite far-fetched, where a user can not control or check each part of the network. In [15] the authors show that this is in fact not necessary, as claims of nonlocality and randomness are robust against the topology of the network. Specifically, as long as a small, 3-party region of the network satisfies the independence assumption, nonlocality can be proven, as well as device-independent randomness on the outcome of the central of the 3 parties. Similar effects have been observed in the quantum steering setting [16].

Here, we propose a DIQKD protocol where all parties in the network perform the same measurement in each

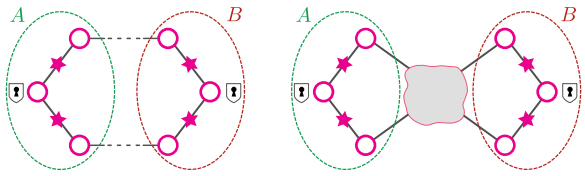

FIG. 1. (a) In order to implement the proposed no-input DIQKD protocol, the users request the distribution of entangled states from sources (stars) in a ring network, which are measured at nodes (circles) using entangling measurements, establishing correlations between Alice's (green) and Bob's (red) labs. The outcomes of the central nodes in the labs can be distilled to a secret key, given that the nodes in-between announce their outcomes. (b) In the security proof Alice and Bob do not assume anything about the structure of the network in-between them, i.e. the rest of the network outside their labs could be collaborating (grey cloud), moreover they do not trust the workings of the independent devices within their own labs either.

round.

Building on the topological robustness results, we require the independence of sources assumptions to only be satisfied within the local neighborhoods of Alice and Bob, in their "labs" (Fig. 1). This is analogous to the independence of the local randomness sources used in conventional DIQKD, where input randomness is necessary, and should be uncorrelated from anything outside the lab. We prove security against collective attacks, and assess how security against general attacks could be proven if the i.i.d. assumption is dropped for the central part of the network.

The manuscript is structured as follows. In Section II, we introduce the protocol, beginning with an illustrative example for the four-party case. Then, we consider scenarios involving semi-trusted and untrusted parties in the network. In Section III we prove the security of the protocol under collective attacks. Finally, in Section IV, we discuss the relevance of the assumptions made and conclude with open questions and possible directions for future research.

II. PROTOCOLS

A. Illustrative Example

We begin by illustrating the protocol in a small network of 4 parties, $\{A_k\}_{k=1}^4$, where only two of them, A_1 and A_3, aim to establish a shared secret key (see Fig. 2). Our DIQKD protocol without inputs goes as follow:

Each source distributes a maximally entangled state

$$\left|\psi^+\right\rangle_{A_k A_{k+1}} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \tag{1}$$

where, by convention, $A_5 \equiv A_1$. Each party then performs a joint RGB4 measurement [7] given by the basis

$$\Big\{ |00\rangle\,,\ u\,|01\rangle + v\,|10\rangle\,, \\ v\,|01\rangle - u\,|10\rangle\,,\ |11\rangle \ \Big|\ u^2+v^2=1,\ u,v\in\mathbb{R}\Big\}, \tag{2}$$

with outcomes labeled as $\{0, 1_L, 1_R, 2\}$. It is convenient to interpret $|0\rangle$ and $|1\rangle$ as the absence or presence of a single excitation. The nonlocality of the resulting distribution can be proven from so-called token counting properties [7, 17]. Specifically, each source can be seen as distributing a single token (excitation) in a superposition, and the measurement can be seen as a counting of the number of incoming tokens, plus outputting some additional coherence information (whether the outcome was 1_L or 1_R). In [14] and later generalized in [15], it is shown that correlations arising from this class of distributions admit self-testing, allowing the underlying quantum realization to be partially certified solely from the observed statistics. This results in the fact that the outcome of any party is non-deterministic from the perspective of an external eavesdropper.

The protocol begins with a stage in which all parties publicly announce the outcomes of the first rounds. These announcements are used to check that the observed statistics are consistent with the RGB4 distribution and, at the same time, serve as a source of public randomness. Even if they respect the RGB4 statistics and we certified that the outcomes are not fully predictable, the adversary may still have partial information about them. Hence, the outcomes of A_1 in these initial rounds can be used as a source of public randomness that is only partially trusted. To remove any potential knowledge that the adversary may have, the randomness is processed via privacy amplification. The resulting secure random bits are then employed to designate the remaining rounds as either verification rounds or key generation rounds. In the verification rounds, as before, all parties reveal their outcomes, and any deviation from the expected RGB4 statistics leads to aborting the protocol.

For the key-generation rounds of our protocol, each party coarse-grains its measurement outcome according to $0, 2 \mapsto 0$ and $1_L, 1_R \mapsto 1$, yielding a binary variable $a_k \in \{0, 1\}$. This procedure produces the outcomes of a single round. This coarse-graining encodes the parity of the total number of excitations detected by a party. Because each entangled source emits exactly one excitation shared between its two adjacent nodes, if one node detects the excitation from a given source, its neighbor necessarily does not. This local exclusivity propagates through the entire chain of sources and imposes a global constraint on the measurement outcomes: the parity of the sum $\sum_k a_k$ is fixed. More precisely, since each excitation is counted exactly once across the network, the sum $\sum_k a_k$ is always even when the number of parties is even, and always odd when the number of parties is odd. In order to generate a key, all parties except those wishing to establish a secret key publicly announce their coarse-grained outcomes; in this case A_2 and A_4 announce. This leads to the parity of $\sum_k a_k - a_1 - a_3$ to be public. Using this information together with their own outcomes and the total parity, the parties A_1 and A_3 can reconstruct the full string of outcomes and thereby establish a shared key bit. For instance, in the first key generation round in Fig. 2, A_1 gets to know $(a_2 = 0, a_4 = 1)$. Knowing that the total parity is 0 and $a_1 = 0$, she can deduce that A_3's coarse-grained outcome must be $a_3 = 1$. Notice that everyone except A_1 and A_3 only has knowledge of the parity of the sum of their two bits.

B. DIQKD protocol in semi-trusted network

We now describe the protocol for a general ring network of N parties, illustrated in Fig. 1(a). Two parties, A_i and A_j, are designated to establish a shared secret key; for convenience, we denote them by $A := A_i$ and $B := A_j$. We consider a scenario in which the local topology around A and B is trusted, i.e., the network structure of the adjacent parties and the sources directly connected

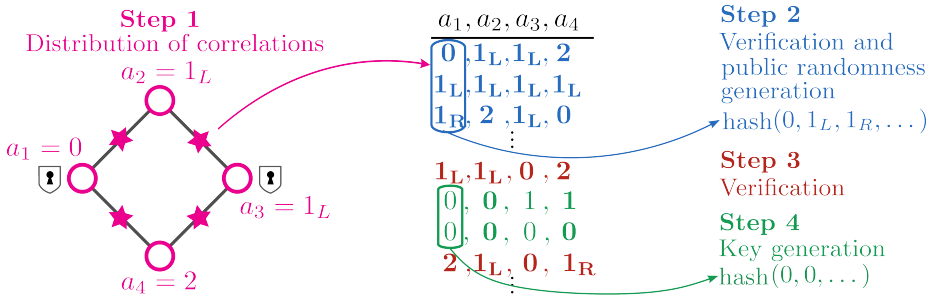

FIG. 2. Overview of the protocol. **Left:** Step 1 (in magenta): The four parties, arranged in a ring network, perform RGB4 measurements on the states they receive, producing coarse-grained outcomes $\{a_k\}_{k=1}^4$. The two parties who will share the final key are indicated with a key symbol. **Middle:** Example outcomes for each party, with publicly announced results in **bold**. **Right:** Step 2 (in blue): Some outcomes are publicly announced to verify RGB4 correlations. A_1's outcomes, after applying a hash H, generate public randomness to determine later rounds as verification or key generation. Step 3 (in red): Verification rounds where all outcomes are revealed to check the RGB4 correlations. Step 4 (in green): Key generation rounds where A_1 and A_3 derive a shared secret key from A_2 and A_4, with hash H applied to the resulting string.

to them is (see Fig. 1.b). Our protocol is secure when the remaining $N-6$ parties do not announce their fine-grained outcomes, hence the phrase semi-trusted. This includes for example the following cases: they are *honest but curious* [18, 19], meaning that they behave honestly during the protocol but try to extract information about the secret key generated by A and B by sharing information about their measurement statistics, or they are *dishonest but isolated*, meaning that they can behave dishonestly during the protocol and lie in their public announcements, but they cannot communicate during the protocol. In that second case, malicious parties can be detected during the verification steps, and the protocol is aborted. The adaptation of our protocol to the case of a fully untrusted network, where dishonest parties are allowed to communicate, is discussed in the next subsection.

The protocol is executed over a total of n rounds. A subset of n_{rand} rounds, corresponding to a fixed fraction of n, is used for distribution verification and public randomness generation. Using the resulting public random string, the remaining $n - n_{\text{rand}}$ rounds are randomly partitioned into n_{test} test rounds and n_{key} key-generation rounds, such that $n = n_{\text{rand}} + n_{\text{test}} + n_{\text{key}}$. The protocol then proceeds as follows:

1. **Distribution of correlations.** In each of the n rounds, the parties $A_1, \ldots, A_N$ each receive two quantum states and perform a local joint RGB4 measurement (Eq. 2), getting values in $\{0, 1_L, 1_R, 2\}$. This step is completed for all n rounds before any outcomes are announced.

2. **Verification and public randomness generation.** The parties publicly announce their outcomes from the first n_{rand} rounds. The protocol is aborted if the observed statistics deviate from the expected distribution. Otherwise, privacy amplification is applied to this string to securely determine which of the remaining rounds are used for key generation and which for testing.

3. **Verification.** All parties reveal their outcomes in the n_{test} test rounds. The protocol is aborted if the observed statistics deviate from the expected distribution.

4. **Key generation.** In the n_{key} key-generation rounds, all parties coarse-grain their outcomes to binary values according to $0, 2 \mapsto 0$ and $1_L, 1_R \mapsto 1$. All parties except A and B announce their outcomes. From their parity, B infers A's raw bit. Party B flips or keeps their bit so that A and B share identical raw keys. Finally, they apply privacy amplification.

Privacy Amplification. (Used in Steps 2, 4.) In the iid setting, each round can be taken as independent from the others, allowing us to partition the rounds in two, resulting in two weak sources of randomness. These can then be used to extract secure randomness. Note that if some randomness is available, for example from Step 1, then other techniques can be used such as families of universal hash functions.

C. Remarks

This protocol allows to generate keys in a ring network in a systematic way, in the sense that all sources generate the same state and all nodes perform the same quantum measurement at every round. Only the classical announcements during the key generation rounds vary depending on which parties decide to generate a secret key. The parties wishing to generate a key can thus reveal themselves only in Step 4, after trust in the network is established.

Note that, in Step 2 and Step 3 of the protocol, the statistics publicly revealed are the outcomes *before*

coarse-graining. This allow the parties to verify that the observed correlations are compatible with the RGB4 distribution. This serves both to detect potential adversarial interventions and errors due to noise. Moreover, as shown in Ref. [15], the outcomes generated in Step 2 cannot be predicted exactly by any external eavesdropper. While an adversary may possess partial information about the raw outcomes, applying privacy amplification ensures that the assignment of rounds becomes arbitrarily random and secure. Similarly, in Step 4, privacy amplification [20] is applied to the raw key produced, guaranteeing that the final key is also random and secure.

Our protocol extends naturally to a *conference key agreement* (CKA) scenario in which a subset of parties $\mathcal{K}$ wish to share a common secret key [21]. To this end, one party $A_1 \in \mathcal{K}$, execute the QKD protocol with each of the other parties $A_j \in \mathcal{K}$, thereby establishing a pairwise secret key with every A_j. These pairwise keys remain secure against all parties outside $\mathcal{K}$. To obtain a single conference key shared by all participants, A_1 publicly announces, for each A_j, the parity between their pairwise key and a designated final key. Since each A_j holds its own pairwise key with A_1, it can reconstruct the final key locally, while parties outside $\mathcal{K}$ cannot infer it.

This construction ensures that all parties in $\mathcal{K}$ obtain the same secret key without leaking any information to non-participating nodes. Moreover, our protocol offers the flexibility for the reference node A_1 to decide each round with whom to generate a secret key bit, while all parties always perform the same quantum operations. While this does not imply a security advantage over other CKA protocols, it might prove more experimentally efficient to implement in a network setting.

D. DIQKD protocol in an untrusted network

We now consider the scenario of a network of N parties in which most nodes are untrusted, as illustrated in Fig. 1(b). As before, two designated parties, A and B, aim to establish a secret key that must remain unknown to both the untrusted nodes and any external eavesdropper. In this setting, the only trusted component of the network is the topology of the sources and parties adjacent to A and B. No trust is placed in the remaining parties, which may behave arbitrarily and even collaborate.

Without coarse-graining the outcomes of the measurement defined in Eq. (2), the parity constraints imply that, after discarding all outcomes equal to 1, the remaining sequence of 0's and 2's on neighboring nodes of the network must alternate. For instance, a local pattern such as 0 2 0 is admissible, whereas two adjacent parties both outputting 0 or both outputting 2 are forbidden.

Because of this alternating structure, a dishonest party that announces the coarse-grained value 0 can still internally distinguish which fine-grained outcome (0 or 2) actually occurred. Moreover, since all untrusted parties can cooperate, they can collectively know the fine-grained outcomes of the entire untrusted region. By combining this knowledge with the coarse-grained announcements of the neighbors of A and B, they can infer the fine-grained outcomes of the two key-generating parties. This leads to a loss of secrecy unless the protocol is appropriately modified.

We now discuss two possible strategies to avoid this leakage. In the first, the protocol proceeds as in Section II B, with a single modification in the key generation step:

4. **Key generation.** All parties except A and B publicly announce their outcomes. Each round is kept only if there exists a sequence of parties connecting the trusted regions of A and B such that all parties along this path announce the coarse-grained value 1; otherwise, the round is discarded. When this condition is satisfied, A and B can infer each other's raw bit using the same parity relations as in the fully trusted case.

Requiring the existence of at least one path of untrusted nodes connecting the trusted regions and outputting the coarse-grained value 1 prevents additional information leakage and ensures that the key remains secure (as 1 is invariant under the coarse-graining). However, this requirement is highly restrictive and significantly suppresses the achievable key rate in larger networks.

A second approach consists in requiring all untrusted nodes to perform entanglement swapping, thereby effectively reducing the network to only the six trusted parties, which then share maximally entangled states. Once this reduction is achieved, the protocol proceeds exactly as in the fully trusted QKD scenario. Any deviation from the prescribed entanglement-swapping operations by an untrusted party is detected during the verification rounds.

This second approach requires a number of entanglement-swapping operations that scales with the number of untrusted nodes, similarly to what would be expected in standard bipartite QKD. While this may be demanding in large networks, the main relevance of both approaches lies in demonstrating that secure key exchange with fixed measurements remains theoretically achievable under suitable structural assumptions, even in the presence of malicious agents.

III. SECURITY PROOF

We now analyze the security properties of our QKD protocol without inputs, in a network of N parties. As introduced in Section II B, two generic parties, denoted A and B, are designated as the key holders.

We prove security under the following assumptions: (i) all N parties share authenticated classical communication channels; (ii) the sources adjacent to A are independent of each other and of the rest of the network (the

same applies to the neighbors of B); (iii) the rounds are independent and identically distributed; (iv) an arbitrarily large number of rounds is performed, so that statistical fluctuations arising from the intrinsic probabilistic nature of the measurement outcomes vanish; (v) quantum states are finite dimensional.

Assumption (i) is common in QKD protocols, since some classical information is typically shared; note, however, that authenticated channels require an initial source of randomness. Assumption (ii) corresponds to the independent-sources model frequently adopted in quantum networks, ensuring that no hidden correlations are introduced through the network; this mirrors the measurement choice independence assumption in Bell nonlocality [22, 23]. Assumption (iii) requires that the rounds are independent and identically distributed, as without it adversaries could exploit memory effects across rounds, reproducing virtually any distribution [24]. Finally, Assumption (iv) places the protocol in the asymptotic regime, allowing one to work directly with the underlying probability distribution without requiring finite-size corrections. Assumption (v) is commonly used in DIQKD proofs for technical reasons. A more detailed discussion of these assumptions is provided in Section IV.

Given these assumptions, we now present the security criterion for the protocol. Let E denote the adversary's quantum register, and focus our analysis on the key generation rounds. In all other rounds, since all measurements are completed before any party makes a public announcement, the only information available to Eve prior to the communication is the outcome of her own measurement device. Security under this condition is guaranteed by [15]. Moreover, the subsequent announcements serve solely to generate public randomness and do not compromise the secrecy of the key. By contrast, in the key generation rounds, any knowledge Eve gains after the announcements could compromise the shared secret key. Therefore, the security analysis must ensure that, even conditioned on her quantum side information and the announcements, Eve's ability to correctly guess the key is strictly bounded. All classical information revealed, including outcomes announced by all parties except A and B during the key generation rounds, is stored in a classical register $\mathcal{P}$.

In the asymptotic i.i.d. regime, security requires that the raw key exhibit intrinsic randomness from the adversary's perspective. This is quantified by the smooth conditional min-entropy $H^{\varepsilon}_{\min}(A|E\mathcal{P})$, which must be strictly positive. In our protocol, the only information about the raw key revealed during key generation rounds is the parity $A\oplus B$, which becomes known once the other parties announce their outcomes. Consequently, the leakage term reduces to a single bit, and it suffices to lower-bound the conditional min-entropy $H^{\varepsilon}_{\min}(A|A\oplus B,E)$.

To this end, we first write explicitly the classical-quantum state shared by the key-generating parties and the adversary after the measurements

$$\rho_{ABE} = \rho_{AE_\alpha} \otimes \rho_{BE_\beta},$$

where the tensor-product structure follows from assumption (ii), the independence of the sources, and E_α (E_β) represents the purifying system of the sources next to A (B) (see Appendix A for details). The effective classical-quantum state describing the state shared by A and E may be written as

$$\rho_{AE} = Q\ |0\rangle\langle 0|_A \otimes \rho_0 + (1-Q)\ |1\rangle\langle 1|_A \otimes \rho_1, \qquad (3)$$

where Q is the probability that the outcome obtained by A is 0, and ρ_0 (resp. ρ_1) denotes the adversary's conditional state when the outcome of A is 0 (resp. $A=1$). Bounding the adversary's knowledge about A therefore reduces to quantifying how well they can distinguish these two conditional states.

Applying the Helstrom bound [25] to Eq. (3) yields the optimal guessing probability for distinguishing the outcomes 0 and 1 of A, which depends solely on the trace distance between the conditional states ρ_0 and ρ_1. A guessing probability strictly smaller than one implies a strictly positive lower bound on the conditional min-entropy $H_{\min}(A|A\oplus B,E)$, and consequently on the smooth min-entropy $H^{\varepsilon}_{\min}(A|A\oplus B,E)$. Such a lower bound can be expressed explicitly, as shown in Appendix A:

$$H^{\varepsilon}_{\min}(A|A\oplus B,E)\ \geq\ -\log_2\left(\frac{1}{2}\sqrt{1-R}\right), \qquad (4)$$

where R is a parameter determined by the RGB4 measurement basis defined in Eq. (2). Optimizing over this parameter, we obtain

$$H^{\varepsilon}_{\min}(A|A\oplus B,E)\ \geq\ 0.1. \qquad (5)$$

In summary, under the stated assumptions, the protocol guarantees that the raw key generated by A and B exhibits intrinsic randomness from the adversary's perspective. The smooth conditional min-entropy $H^{\varepsilon}_{\min}(A|A\oplus B,E)$ is strictly positive, which implies that a secret key can be securely extracted. This establishes the security of the key generation in our QKD protocol without inputs.

IV. DISCUSSION AND OPEN QUESTIONS

We conclude by discussing several conceptual aspects of our framework and outlining directions for future work.

Assumption (i) requires the parties to share authenticated classical communication channels, as is standard in network-assisted quantum cryptography. Authentication typically consumes a small initial amount of randomness shared between the two parties. This cost is negligible in practice since a new shared key is being generated whose size is linear in the number of rounds, whereas the classical authentication requires a shared key that is logarithmic in the message size. Hence, after kick-starting the algorithm, authentication is easily handled.

Assumption (iv) places our protocol in the asymptotic regime of infinitely many rounds. Although any practical implementation will necessarily operate with a finite

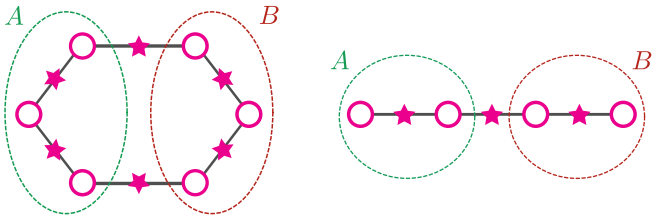

FIG. 3. Comparison between our network (left) and the four-party line network (right) known to be equivalent to the standard Bell scenario [5]. In each case, the nodes corresponding to the effective "Alice" and "Bob" are highlighted.

number of rounds, the asymptotic limit is invoked here primarily to make a conceptual point: even in the complete absence of externally supplied input randomness, it is in principle possible to generate and certify randomness solely from the intrinsic structure of the network and the observed output statistics. Developing a finite-round analysis for this input-free setting is an important but separate challenge for future work.

We also comment briefly on the role of the seed S_{test} used to designate test rounds. In the protocol we adopt the simplest possible implementation, where each bit of S_{test} acts as a binary flag distinguishing test from generation rounds. More elaborate strategies are possible—for instance, grouping several bits into an integer that determines in how many rounds the next test occurs, thereby yielding sparser or irregularly spaced testing patterns.

It is instructive to compare our network-based framework with the standard Bell-nonlocality setting (see Fig. 3). In a Bell test, one studies behaviours $\{p(ab|xy)\}_{a,b,x,y}$, where the inputs x and y must be chosen freely—namely, independently of any shared past or adversarial system—to avoid locality and measurement-independence loopholes. From a network perspective, however, these "free" inputs can themselves be generated by additional parties in a larger correlation scenario. Indeed, as shown in [5], the usual Bell scenario is equivalent to a four-party line-network in which the inputs arise as outcomes of the two outer nodes. Under this equivalence, the standard Bell assumptions (including measurement independence) translate directly into an *independent-sources* assumption in the network. This observation clarifies that the independence requirement on the sources in our framework is not a stronger assumption than those made in Bell experiments; rather, it is the natural network-theoretic analogue of the measurement-independence condition that underlies all device-independent protocols.

The analysis in Ref. [24] pinpoints an issue that is crucial in networks with no inputs - namely that the i.i.d. assumption can not be left away without introducing a memory loophole. Given the equivalence of standard Bell nonlocality to a no-input line network scenario (Fig. 3b), one may ask why the memory loophole does not appear there. In non-iid QKD security proofs one assumes a lower bound on the quality of the input randomness, implying that it cannot completely be controlled or pre-programmed by an adversary. Typically, one assumes an iid property for the input randomness, with only recent attempts to relax this [26, 27]. In our network setup, due to the memory loophole, we only have the possibility to completely relax the iid assumption of one source. Thus, a natural choice is to keep the iid assumption on Alice and Bob's immediate neighborhood, which one can imagine as their laboratories, leaving the rest of the network, the untrusted center, to be non-iid. It is yet unclear how much the iid assumption on the labs can be relaxed, analogously to [26, 27], if at all. Presumably the most straight-forward way would be to generalize the results of [14, 15] by giving a robust bound for the min entropy, even under noisy realizations of the ideal distribution. Then the generalized entropy accumulation theorem may be applicable, similarly as in [28]. This is left for future work.

Finally, note that any randomness that we use as input in our protocol, namely for authentication, can be generated before starting the protocol. Indeed, even in standard DIQKD, the parties must come together physically in order to establish a shared random seed that they use for authentication. This is the case also for us; and when they come together in an isolated lab, they can run only Step 1 of our protocol (or equivalently, the randomness certification in Ref. [14]) to obtain the random seed with no inputs used. This allows our no input (fixed measurement setting) protocol to be a protocol which requires no input randomness at all. Note however, that this technique could also render standard DIQKD to be operated without any randomness as an input.

V. CONCLUSION

In summary, we have introduced protocols for quantum key distribution and conference key agreement in network scenarios that does not rely on local input randomness. By performing pre-decided measurements at each node and exploiting the structure of the network, we showed that it is possible to establish secret keys even when most nodes and sources are untrusted. This approach preserves the essential device-independent features of Bell inequality-based protocols while introducing a natural network-theoretic perspective on assumptions such as source independence.

Future work could investigate finite-round analyses, strategies for optimized selection of test rounds, and alternative network assumptions to further relax the trust requirements.

[1] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, *et al.*, Advances in quantum cryptography, Advances in optics and photonics **12**, 1012 (2020).

[2] V. Zapatero, T. van Leent, R. Arnon-Friedman, W.-Z. Liu, Q. Zhang, H. Weinfurter, and M. Curty, Advances in device-independent quantum key distribution, npj quantum information **9**, 10 (2023).

[3] C. Branciard, N. Gisin, and S. Pironio, Characterizing the nonlocal correlations created via entanglement swapping, Phys. Rev. Lett. **104**, 170401 (2010).

[4] C. Branciard, D. Rosset, N. Gisin, and S. Pironio, Bilocal versus nonbilocal correlations in entanglement-swapping experiments, Phys. Rev. A **85**, 032119 (2012).

[5] T. Fritz, Beyond bell's theorem: correlation scenarios, New Journal of Physics **14**, 103001 (2012).

[6] A. Tavakoli, A. Pozas-Kerstjens, M.-X. Luo, and M.-O. Renou, enBell nonlocality in networks, Reports on Progress in Physics **85**, 056001 (2022).

[7] M.-O. Renou, E. Bäumer, S. Boreiri, N. Brunner, N. Gisin, and S. Beigi, Genuine quantum nonlocality in the triangle network, Physical review letters **123**, 140401 (2019).

[8] P. Abiuso, T. Kriváchy, E.-C. Boghiu, M.-O. Renou, A. Pozas-Kerstjens, and A. Acín, Single-photon nonlocality in quantum networks, Phys. Rev. Res. **4**, L012041 (2022).

[9] T. Kriváchy and M. Kerschbaumer, Closing the detection loophole in the triangle network with high-dimensional photonic states, Phys. Rev. Lett. **135**, 160803 (2025).

[10] O. Meskine, I. Šupić, D. Markham, F. Appas, F. Boitier, M. Morassi, A. Lemaître, M. Amanti, F. Baboux, E. Diamanti, and S. Ducci, Experimental fiber-based quantum triangle-network nonlocality with a telecom AlGaAs multiplexed entangled-photon source, PRX Quantum **6**, 020313 (2025).

[11] N.-N. Wang, C. Zhang, H. Cao, K. Xu, B.-H. Liu, Y.-F. Huang, C.-F. Li, G.-C. Guo, N. Gisin, T. Kriváchy, and M.-O. Renou, Experimental genuine quantum nonlocality in the triangle network (2024), arXiv:2401.15428 [quant-ph].

[12] E. Polino, D. Poderini, G. Rodari, I. Agresti, A. Suprano, G. Carvacho, E. Wolfe, A. Canabarro, G. Moreno, G. Milani, *et al.*, Experimental nonclassicality in a causal network without assuming freedom of choice, Nature Communications **14**, 909 (2023).

[13] S. Sarkar, Network quantum steering enables randomness certification without seed randomness, Quantum **8**, 1419 (2024).

[14] P. Sekatski, S. Boreiri, and N. Brunner, Partial self-testing and randomness certification in the triangle network, Phys. Rev. Lett. **131**, 100201 (2023).

[15] S. Boreiri, T. Kriváchy, P. Sekatski, A. Girardin, and N. Brunner, Topologically robust quantum network nonlocality, Physical Review Letters **134**, 010202 (2025).

[16] D. Baheti and S. Sarkar, Topologically noise-robust network steering without inputs, Phys. Rev. A **113**, 012607 (2026).

[17] M.-O. Renou and S. Beigi, Network nonlocality via rigidity of token counting and color matching, Physical Review A **105**, 022408 (2022).

[18] A. Cojocaru, L. Colisson, E. Kashefi, and P. Wallden, On the possibility of classical client blind quantum computing, Cryptography **5**, 3 (2021).

[19] E. Kashefi and P. Wallden, Garbled quantum computation, Cryptography **1**, 6 (2017).

[20] R. Renner and R. König, Universally composable privacy amplification against quantum adversaries, in *Theory of Cryptography Conference* (Springer, 2005) pp. 407–425.

[21] G. Murta, F. Grasselli, H. Kampermann, and D. Bruß, Quantum conference key agreement: A review, Advanced Quantum Technologies **3**, 2000025 (2020).

[22] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Reviews of modern physics **86**, 419 (2014).

[23] M. J. Hall, The significance of measurement independence for bell inequalities and locality, in *At the Frontier of Spacetime: Scalar-Tensor Theory, Bells Inequality, Machs Principle, Exotic Smoothness* (Springer, 2016) pp. 189–204.

[24] M. Weilenmann, C. Budroni, and M. Navascues, Memory attacks in network nonlocality and self-testing, Quantum **9**, 1735 (2025).

[25] C. W. Helstrom, Quantum detection and estimation theory, Journal of Statistical Physics **1**, 231 (1969).

[26] M. Kessler and R. Arnon-Friedman, Device-independent randomness amplification and privatization, IEEE Journal on Selected Areas in Information Theory **1**, 568 (2020).

[27] M. Sandfuchs, C. Ferradini, and R. Renner, Randomness from causally independent processes (2025), arXiv:2510.05203 [quant-ph].

[28] T. Metger and R. Renner, Security of quantum key distribution from generalised entropy accumulation, Nature Communications **14**, 5272 (2023).

[29] M. Tomamichel, R. Colbeck, and R. Renner, A fully quantum asymptotic equipartition property, IEEE Transactions on Information Theory **55** (2009).

Appendix A: Security Proof

To certify the length l of bits that we can extract in a protocol we can use the leftover hash lemma (LHL), that in presence of an adversary E and some public announcements $\mathcal{P}$ is written as

$$l \leq \left\lfloor H_{\min}^{\varepsilon}(A|E) - \text{leak}_{\text{KG}} - 2\log\left(\frac{1}{\varepsilon'}\right)\right\rfloor, \tag{A1}$$

where $H_{\min}^{\varepsilon}$ is the smooth min entropy, A is the register of the key, E is the register of information held by the external eavesdropper and leak_{KG} is the leakage of information due to the announcements $\mathcal{P}$. Using the results in ... we can upper bound $H_{\min}^{\varepsilon}(A|E) - \text{leak}_{\text{KG}}$ as

$$H_{\min}^{\varepsilon}(A|E) - \text{leak}_{\text{KG}} \leq H_{\min}^{\varepsilon}(A|E\mathcal{P}). \tag{A2}$$

To bound the smooth min-entropy, we apply the quantum asymptotic equipartition property (QAEP) [29, Thm. 9]

$$H_{\min}^{\varepsilon}(A \mid E\mathcal{P}) \geq k\, H(a \mid E\mathcal{P}_{\text{round}}) - \sqrt{k}\,\delta(\varepsilon,\eta), \tag{A3}$$

where k is the length of the raw key, a is the outcome of a single round, and $\mathcal{P}_{\text{round}}$ denotes the classical information leaked during that round.

Using the standard relation between von Neumann and min-entropy, this can be further lower-bounded as

$$H_{\min}^{\varepsilon}(A \mid E\mathcal{P}) \geq k\, H_{\min}(a \mid E\mathcal{P}_{\text{round}}) - \sqrt{k}\,\delta(\varepsilon,\eta). \tag{A4}$$

Finally, noting that the conditional min-entropy is related to the adversary's guessing probability via

$$H_{\min}(a|E\mathcal{P}_{\text{round}}) = -\log p_{\text{guess}}(a|E\mathcal{P}_{\text{round}}), \tag{A5}$$

the problem reduces to bounding the guessing probability of the raw key bits. The scenario under consideration is illustrated in Fig. 4.

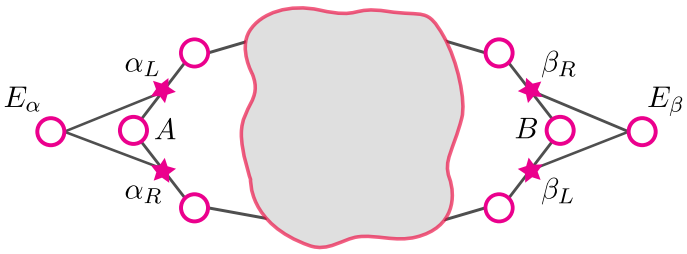

FIG. 4. The adversary E is correlated with the sources adjacent to the key-generating parties A and B. The remaining parties, represented by the cloud, are untrusted.

To this end, we adapt the proof of Theorem 7 in [15] to our setting, which additionally includes some classical public announcements. The corresponding global state of parties A, B, and the adversary E reads

$$\begin{aligned}
&\varphi_{ABE} = \rho_{AE_{\alpha_L}E_{\alpha_R}} \otimes \sigma_{BE_{\beta_L}E_{\beta_R}} = \\
&\Big[|0\rangle\langle 0|_A \left(p_{\alpha_R}(1-p_{\alpha_L})\rho^1_{E_{\alpha_L}}\rho^1_{E_{\alpha_R}} + p_{\alpha_L}(1-p_{\alpha_R})\rho^0_{E_{\alpha_L}}\rho^0_{E_{\alpha_R}}\right) \\
&+ |1\rangle\langle 1|_A \left(p_{\alpha_R}p_{\alpha_L}\rho^0_{E_{\alpha_L}}\rho^1_{E_{\alpha_R}} + (1-p_{\alpha_L})(1-p_{\alpha_R})\rho^1_{E_{\alpha_L}}\rho^0_{E_{\alpha_R}}\right)\Big] \\
&\otimes \Big[|0\rangle\langle 0|_B \left(p_{\beta_R}(1-p_{\beta_L})\sigma^1_{E_{\beta_L}}\sigma^1_{E_{\beta_R}} + p_{\beta_L}(1-p_{\beta_R})\sigma^0_{E_{\beta_L}}\sigma^0_{E_{\beta_R}}\right) \\
&+ |1\rangle\langle 1|_B \left(p_{\beta_R}p_{\beta_L}\sigma^0_{E_{\beta_L}}\sigma^1_{E_{\beta_R}} + (1-p_{\beta_L})(1-p_{\beta_R})\sigma^1_{E_{\beta_L}}\sigma^0_{E_{\beta_R}}\right)\Big],
\end{aligned} \tag{A6}$$

where $p_{\alpha_L}, p_{\alpha_R}, p_{\beta_L}, p_{\beta_R}$ denote the probabilities that the sources α_L, α_R, β_L, and β_R send the excitation to the left. For α_L and β_L, this corresponds to sending the excitation away from the party, whereas for α_R and β_R it corresponds to sending the excitation toward the party.

The states $\rho^1_{E_i}$ and $\rho^0_{E_i}$ (and analogously $\sigma^1_{E_i}$ and $\sigma^0_{E_i}$) describe the quantum state held by the adversary E, conditioned on whether the excitation reaches party A or not, respectively (and analogously party B in the case of σ), and originating from the source i. We assume that the states held by the adversary corresponding to different sources are separable given the assumption of source independence.

The states observed by parties A and B are coarse-grained into binary outcomes 0 and 1. The outcome 0 corresponds to the event of receiving either one token from both sources (fine-grained outcome 2) or no token from either source (fine-grained outcome 0). Similarly, the outcome 1 corresponds to receiving exactly one token from one of the sources (fine-grained outcomes 1_L and 1_R).

To incorporate the publicly announced information, we may introduce an auxiliary register $A \oplus B$ and apply a unitary channel U defined as

$$U: \ |a\rangle_A |b\rangle_B |0\rangle_{A\oplus B} \ \longrightarrow \ |a\rangle_A |b\rangle_B |a \oplus b\rangle_{A\oplus B}, \tag{A7}$$

which stores this extra information inside the state. Since we are ultimately interested only in the outcomes held by party A, we may subsequently trace out subsystem B. Explicitly, the global state becomes

$$\begin{aligned}
&\rho_{A,A\oplus B,E} = \mathrm{Tr}_B[U(\varphi_{ABE} \otimes |0\rangle\langle 0|_{A\oplus B})U^\dagger] = \\
&|0\rangle\langle 0|_A \otimes \Big[|0\rangle\langle 0|_{A\oplus B} p_{\alpha_R}(1-p_{\alpha_L})p_{\beta_R}(1-p_{\beta_L})\rho^{11}\sigma^{11} + |0\rangle\langle 0|_{A\oplus B} p_{\alpha_R}(1-p_{\alpha_L})p_{\beta_L}(1-p_{\beta_R})\rho^{11}\sigma^{00} \\
&\quad + |0\rangle\langle 0|_{A\oplus B} p_{\alpha_L}(1-p_{\alpha_R})p_{\beta_R}(1-p_{\beta_L})\rho^{00}\sigma^{11} + |0\rangle\langle 0|_{A\oplus B} p_{\alpha_L}(1-p_{\alpha_R})p_{\beta_L}(1-p_{\beta_R})\rho^{00}\sigma^{00} \\
&\quad + |1\rangle\langle 1|_{A\oplus B} p_{\alpha_R}(1-p_{\alpha_L})p_{\beta_R}p_{\beta_L}\rho^{11}\sigma^{01} + |1\rangle\langle 1|_{A\oplus B} p_{\alpha_R}(1-p_{\alpha_L})(1-p_{\beta_L})(1-p_{\beta_R})\rho^{11}\sigma^{10} \\
&\quad + |1\rangle\langle 1|_{A\oplus B} p_{\alpha_L}(1-p_{\alpha_R})p_{\beta_R}p_{\beta_L}\rho^{00}\sigma^{01} + |1\rangle\langle 1|_{A\oplus B} p_{\alpha_L}(1-p_{\alpha_R})(1-p_{\beta_L})(1-p_{\beta_R})\rho^{00}\sigma^{10}\Big] \\
+&|1\rangle\langle 1|_A \otimes \Big[|0\rangle\langle 0|_{A\oplus B} p_{\alpha_R}p_{\alpha_L}p_{\beta_R}p_{\beta_L}\rho^{01}\sigma^{01} + |0\rangle\langle 0|_{A\oplus B} p_{\alpha_R}p_{\alpha_L}(1-p_{\beta_L})(1-p_{\beta_R})\rho^{01}\sigma^{10} \\
&\quad + |0\rangle\langle 0|_{A\oplus B} (1-p_{\alpha_R})(1-p_{\alpha_L})p_{\beta_R}p_{\beta_L}\rho^{10}\sigma^{01} + |0\rangle\langle 0|_{A\oplus B} (1-p_{\alpha_R})(1-p_{\alpha_L})(1-p_{\beta_L})(1-p_{\beta_R})\rho^{10}\sigma^{10} \\
&\quad + |1\rangle\langle 1|_{A\oplus B} p_{\alpha_R}p_{\alpha_L}p_{\beta_R}(1-p_{\beta_L})\rho^{01}\sigma^{11} + |1\rangle\langle 1|_{A\oplus B} p_{\alpha_R}p_{\alpha_L}p_{\beta_L}(1-p_{\beta_R})\rho^{01}\sigma^{00} \\
&\quad + |1\rangle\langle 1|_{A\oplus B} (1-p_{\alpha_R})(1-p_{\alpha_L})p_{\beta_R}(1-p_{\beta_L})\rho^{10}\sigma^{11} + |1\rangle\langle 1|_{A\oplus B} (1-p_{\alpha_R})(1-p_{\alpha_L})p_{\beta_L}(1-p_{\beta_R})\rho^{10}\sigma^{00}\Big],
\end{aligned} \tag{A8}$$

where $\rho^{ij} = \rho^i_{E_{\alpha_R}} \otimes \rho^j_{E_{\alpha_L}}$ and $\sigma^{ij} = \sigma^i_{E_{\beta_R}} \otimes \sigma^j_{E_{\beta_L}}$ $\forall i,j \in \{0,1\}$. Eq. (A8) can be written in a more compact way as

$$\phi_{A,A\oplus B,E} = Q\,|0\rangle\langle 0|_A \otimes \tau^0_{A\oplus B,E} + (1-Q)\,|1\rangle\langle 1|_A \otimes \tau^1_{A\oplus B,E}, \tag{A9}$$

where

$$\tau^0_{A\oplus B,E} = \frac{|0\rangle\langle 0|_{A\oplus B} \otimes \rho^0_E\sigma^0_E + |1\rangle\langle 1|_{A\oplus B} \otimes \rho^0_E\sigma^1_E}{Q}, \quad \tau^1_{A\oplus B,E} = \frac{|0\rangle\langle 0|_{A\oplus B} \otimes \rho^1_E\sigma^1_E + |1\rangle\langle 1|_{A\oplus B} \otimes \rho^1_E\sigma^0_E}{1-Q}. \tag{A10}$$

The conditional states of Eve are given by

$$\begin{aligned}
\rho^0_E &= p_{\alpha_R}(1-p_{\alpha_L})\,\rho^{01}_{E_{\alpha_L}} \otimes \rho^{10}_{E_{\alpha_R}} + p_{\alpha_L}(1-p_{\alpha_R})\,\rho^{10}_{E_{\alpha_L}} \otimes \rho^{01}_{E_{\alpha_R}}, \\
\rho^1_E &= p_{\alpha_R}p_{\alpha_L}\,\rho^{10}_{E_{\alpha_L}} \otimes \rho^{10}_{E_{\alpha_R}} + (1-p_{\alpha_L})(1-p_{\alpha_R})\,\rho^{01}_{E_{\alpha_L}} \otimes \rho^{01}_{E_{\alpha_R}}, \\
\sigma^0_E &= p_{\beta_R}(1-p_{\beta_L})\,\rho^{01}_{E_{\beta_L}} \otimes \rho^{10}_{E_{\beta_R}} + p_{\beta_L}(1-p_{\beta_R})\,\rho^{10}_{E_{\beta_L}} \otimes \rho^{01}_{E_{\beta_R}}, \\
\sigma^1_E &= p_{\beta_R}p_{\beta_L}\,\rho^{10}_{E_{\beta_L}} \otimes \rho^{10}_{E_{\beta_R}} + (1-p_{\beta_L})(1-p_{\beta_R})\,\rho^{01}_{E_{\beta_L}} \otimes \rho^{01}_{E_{\beta_R}}.
\end{aligned} \tag{A11}$$

The coefficient Q is defined as

$$Q = \sum_{\substack{s_1,s_2=1-s_1,\\ s_3,s_4\in\{0,1\}}} p^{s_1}_{\alpha_L}(1-p_{\alpha_L})^{1-s_1}p^{s_2}_{\alpha_R}(1-p_{\alpha_R})^{1-s_2}p^{s_3}_{\beta_L}(1-p_{\beta_L})^{1-s_3}p^{s_4}_{\beta_R}(1-p_{\beta_R})^{1-s_4}. \tag{A12}$$

This expression follows from the observation that, when the outcome of A is $|0\rangle_A$, either both excitations from the adjacent sources are detected by A or neither is detected. Consequently, the corresponding probabilities necessarily appear in combinations of the form $p_{\alpha_i}(1-p_{\alpha_j})$ with $i,j \in \{L,R\}$ and $i \neq j$. This constraint is enforced in Eq. (A12) by imposing the condition $s_2 = 1-s_1$ in the summation.

Now we can apply the Holevo-Helstrom theorem to the state $\phi_{A,A\oplus B,E}$

$$p_g(A|A\oplus B,E) \leq \frac{1}{2}\left(1+\left|\left|Q\tau^0_{A\oplus B,E}-(1-Q)\tau^1_{A\oplus B,E}\right|\right|_1\right), \tag{A13}$$

where $||\cdot||_1$ denotes the trace norm. We can bound the trace distance between two subnormalized states as

$$||p\omega - q\tau||_1 \leq \sqrt{(p+q)^2-4pqF(\omega,\tau)}, \tag{A14}$$

thus obtaining

$$\begin{aligned}
p_g(A|A\oplus B,E) \leq \frac{1}{2}\Big[1+ \\
&+(1-p_{\alpha_L})\sqrt{(1-p_{\alpha_R}-p_{\beta_R}+2p_{\alpha_R}p_{\beta_R})^2-4p_{\alpha_R}p_{\beta_R}(1-p_{\alpha_R})(1-p_{\beta_R})F_{\alpha_R}F_{\beta_R}} \\
&+p_{\alpha_R}\sqrt{(1-p_{\alpha_L}-p_{\beta_R}+2p_{\alpha_L}p_{\beta_R})^2-4p_{\alpha_L}p_{\beta_R}(1-p_{\alpha_L})(1-p_{\beta_R})F_{\alpha_L}F_{\beta_R}} \\
&+|(1-p_{\alpha_R})p_{\beta_R}|\left(\sqrt{(p_{\alpha_L}+p_{\beta_L}-2p_{\alpha_L}p_{\beta_L})^2-4p_{\alpha_L}p_{\beta_L}(1-p_{\alpha_L})(1-p_{\beta_L})F_{\alpha_L}F_{\beta_L}}\right. \\
&\left.+\sqrt{(1-p_{\alpha_L}-p_{\beta_L}+2p_{\alpha_L}p_{\beta_L})^2-4p_{\alpha_L}p_{\beta_L}(1-p_{\alpha_L})(1-p_{\beta_L})F_{\alpha_L}F_{\beta_L}}\right) \\
&+|p_{\alpha_L}(1-p_{\beta_R})|\left(\sqrt{(1-p_{\alpha_R}-p_{\beta_L}+2p_{\alpha_R}p_{\beta_L})^2-4p_{\alpha_R}p_{\beta_L}(1-p_{\alpha_R})(1-p_{\beta_L})F_{\alpha_R}F_{\beta_L}}\right. \\
&\left.+\sqrt{(p_{\alpha_R}+p_{\beta_L}-2p_{\alpha_R}p_{\beta_L})^2-4p_{\alpha_R}p_{\beta_L}(1-p_{\alpha_R})(1-p_{\beta_L})F_{\alpha_R}F_{\beta_L}}\right)\Big].
\end{aligned}$$

For $p_{\alpha_L}=p_{\alpha_R}=p_{\beta_L}=p_{\beta_R}=1/2$ it becomes

$$\begin{aligned}
p_g(A|A\oplus B,E) \leq \frac{1}{2}\Big[1+\frac{1}{4}\Big(&\sqrt{1-F_{\alpha_R}F_{\beta_R}}+\sqrt{1-F_{\alpha_L}F_{\beta_R}}+ \\
&+\sqrt{1-F_{\alpha_L}F_{\beta_L}}+\sqrt{1-F_{\alpha_R}F_{\beta_L}}\Big)\Big].
\end{aligned} \tag{A15}$$

In the scenario considered in this manuscript, we have $p_{\alpha_L}=p_{\alpha_R}=p_{\beta_L}=p_{\beta_R}=1/2$, and therefore

$$p_g(A|A\oplus B,E) \leq \frac{1}{2}\left[1+\frac{1}{4}\left(\sqrt{1-F_{\alpha_R}F_{\beta_R}}+\sqrt{1-F_{\alpha_L}F_{\beta_R}}+\sqrt{1-F_{\alpha_L}F_{\beta_L}}+\sqrt{1-F_{\alpha_R}F_{\beta_L}}\right)\right]. \tag{A16}$$

Following the approach in [15], we introduce the *global coherence factor* R [15, Thm. 6]. The bound given for the global coherence parameter applies both for Alice and for Bob, which when multiplied, give the constraint

$$F_{\alpha_R}F_{\alpha_L}F_{\beta_R}F_{\beta_L} \geq R^2. \tag{A17}$$

Now we can analytically find the maximum for the upper bound to $p_g(A|A\oplus B,E)$ given by Eq. (A16) under the constraint in Eq. (A17). Assume that the maximum is attained at $(F^*_{\alpha_R},F^*_{\alpha_L},F^*_{\beta_R},F^*_{\beta_L})$ with $F^*_{\alpha_R}<F^*_{\alpha_L}$. Now consider the value of the function at a slightly perturbed point

$$\begin{aligned}
&f(F^*_{\alpha_R}+\delta,F^*_{\alpha_L}-\delta,F^*_{\beta_R},F^*_{\beta_L}) = \\
&\frac{1}{2}\left[1+\frac{1}{4}\left(\sqrt{1-(F^*_{\alpha_R}+\delta)F^*_{\beta_R}}+\sqrt{1-(F^*_{\alpha_L}-\delta)F^*_{\beta_R}}+\sqrt{1-F^*_{\alpha_L}F^*_{\beta_L}}+\sqrt{1-F^*_{\alpha_R}F^*_{\beta_L}}\right)\right] = \\
&\frac{1}{2}\left[1+\frac{1}{4}\left(\sqrt{1-F^*_{\alpha_R}F^*_{\beta_R}-\delta F^*_{\beta_R}}+\sqrt{1-F^*_{\alpha_L}F^*_{\beta_R}+\delta F^*_{\beta_R}}+\sqrt{1-F^*_{\alpha_L}F^*_{\beta_L}}+\sqrt{1-F^*_{\alpha_R}F^*_{\beta_L}}\right)\right].
\end{aligned} \tag{A18}$$

It is easy to see that for δ small enough, the fidelities still belong to $[0,1]$, and moreover, the constraint $F_{\alpha_R}F_{\alpha_L}F_{\beta_R}F_{\beta_L}\geq R^2$ is also satisfied

$$(F^*_{\alpha_R}+\delta)(F^*_{\alpha_L}-\delta)F^*_{\beta_R}F^*_{\beta_L} = F^*_{\alpha_R}F^*_{\alpha_L}F^*_{\beta_R}F^*_{\beta_L}+\delta F^*_{\alpha_L}F^*_{\beta_R}F^*_{\beta_L}-\delta F^*_{\alpha_R}F^*_{\beta_R}F^*_{\beta_L}-\delta^2F^*_{\beta_R}F^*_{\beta_L} \geq R^2. \tag{A19}$$

In Eq. (A18), it holds that $\sqrt{a-\delta}+\sqrt{b+\delta} > \sqrt{a}+\sqrt{b}$ for $a > b$ and sufficiently small δ, as can be seen from the Taylor expansion of the square root

$$\sqrt{a-x}+\sqrt{b+x} \overset{T}{\sim} \sqrt{a}-\frac{x}{2a}+\sqrt{b}+\frac{x}{2b}\bigg|_{a>b} > \sqrt{a}+\sqrt{b}, \tag{A20}$$

where $\overset{\mathrm{T}}{\sim}$ denotes the first-order Taylor expansion. It follows that

$$f(F^*_{\alpha_R}+\delta, F^*_{\alpha_L}-\delta, F^*_{\beta_R}, F^*_{\beta_L}) > f(F^*_{\alpha_R}, F^*_{\alpha_L}, F^*_{\beta_R}, F^*_{\beta_L}), \tag{A21}$$

which contradicts the assumption that the latter point was optimal. Due to the symmetry of the function under swapping F_{α_R} and F_{α_L}, the same contradiction arises if $F^*_{\alpha_R} > F^*_{\alpha_L}$. An analogous argument holds for $F^*_{\beta_R}$ and $F^*_{\beta_L}$. Hence, the maximum is attained at

$$F^*_{\alpha_R} = F^*_{\alpha_L} \quad \text{and} \quad F^*_{\beta_R} = F^*_{\beta_L}. \tag{A22}$$

Since the function is continuous and defined over a compact domain, a maximum must exist, and from the above symmetry argument, it must occur at

$$f(F^*_{\alpha_R} = F^*_{\alpha_L}, F^*_{\beta_R} = F^*_{\beta_L}) = \frac{1}{2}\left[1+\sqrt{1-F^*_{\alpha_R}F^*_{\beta_R}}\right]. \tag{A23}$$

From the constraint $(F^*_{\alpha_R}F^*_{\beta_R})^2 \geq R^2$, it follows that the maximum value is $\max f = \frac{1}{2}\left[1+\sqrt{1-R}\right]$, meaning that the complete expression for the min-entropy is

$$H_{\min}(a|E\mathcal{P}_{\text{round}}) \geq -\log\left[\frac{1}{2}\left(1+\sqrt{1-R}\right)\right] = 1-\log\left(1+\sqrt{1-R}\right). \tag{A24}$$