Conference key agreement with single-photon interference

Federico Grasselli, Hermann Kampermann and Dagmar Bruß
Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstraße 1, D-40225, Düsseldorf, Germany
E-mail: federico.grasselli@hhu.de

Keywords: multipartite QKD, single-photon interference, conference key agreement, W-state, finite-key, TF-QKD

Abstract

The intense research activity on Twin-Field (TF) quantum key distribution (QKD) is motivated by the fact that two users can establish a secret key by relying on single-photon interference in an untrusted node. Thanks to this feature, variants of the protocol have been proven to beat the point-to-point private capacity of a lossy quantum channel. Here we generalize the main idea of the TF-QKD protocol introduced by Curty et al to the multipartite scenario, by devising a conference key agreement (CKA) where the users simultaneously distill a secret conference key through single-photon interference. The new CKA is better suited to high-loss scenarios than previous multipartite QKD schemes and it employs for the first time a W-class state as its entanglement resource. We prove the protocol’s security in the finite-key regime and under general attacks. We also compare its performance with the iterative use of bipartite QKD protocols and show that our truly multipartite scheme can be advantageous, depending on the loss and on the state preparation.

The most mature and developed application of quantum communication [1, 2] is certainly quantum key distribution (QKD) [3–8]. The majority of the QKD protocols proposed so far involve just two end-users, Alice and Bob, who want to establish a secret shared key. Nowadays there is a vibrant research towards protocols which are proven to be secure in the most adversarial situation possible (i.e. reducing the assumption on the devices) [9–14], but at the same time are also implementable with today’s technology [15–18]. In this context, a protocol which recently received great attention is the Twin-Field (TF) QKD protocol originally proposed by Lucamarini et al [19], further developed to prove its security [20–27] and experimentally implemented [28–31]. Indeed, the TF-QKD protocol relies only on single-photon interference occurring in an untrusted node, making it a measurement-device-independent (MDI) QKD protocol capable of overcoming the repeaterless bounds [32, 33].

In a scenario where several users are required to share a common secret key, one can for instance perform bipartite QKD protocols between pairs of users and then use the secret keys established in this way to encode the final common secret key. Alternatively, one can perform a truly multipartite QKD scheme—also known as conference key agreement (CKA)—whose purpose is to deliver the same secret key to all the parties involved in the protocol [35–39]. In order to accomplish such a task, a resource which seems necessary is the multipartite Greenberger–Horne–Zeilinger (GHZ) state [34–38] or a multipartite private state—a ‘twisted’ version of the GHZ state [40, 41].

In this work we introduce a CKA which exploits for the first time the multipartite entanglement of a W-class state [42], in order to deliver the same secret key to all users. Despite having a number of users involved, the scheme relies on single-photon interference in an untrusted node and it is inspired by the bipartite TF-QKD protocol by Curty et al [24]. We prove the security of our CKA in the finite-key scenario, allowing Eve to perform the most general attacks (coherent attacks) on the transmitted signals. We compare the performance of our genuinely multipartite QKD scheme with the iterative use of bipartite QKD protocols, both in the asymptotic regime and in the finite-key regime. In doing so, we show that performing a truly multipartite scheme can yield a higher secret key rate, depending on the loss and on the state preparation.

The paper is structured as follows. In section 1 we present the CKA based on single-photon interference, while in section 2 we discuss the establishment of a secret conference key where the entanglement resource is a W-class state.
state. In section 3 we prove the CKA security in the finite-key scenario (the detailed proof is given in appendix A). In section 4 we provide simulations of the protocol’s secret key rate and compare them with the repeated use of bipartite schemes (further comparisons in appendix C). We present our conclusions in section 5. In appendix B we report in detail the calculations of the relevant parameters for an honest implementation of the protocol.

1. Conference key agreement

As anticipated in the introduction, our CKA scheme is an extension of the original bipartite TF-QKD protocol [24], Protocol 1 to a scenario with \( N \) users who want to establish a secret conference key. The parties distill the secret key by sending optical pulses to an untrusted node and by performing suitable measurements on a qubit they hold. In order to keep the notation symmetric, the \( N \) parties involved in the multipartite QKD protocol are named: Alice, Alice\(_1\), ..., Alice\(_N\). The protocol is composed of \( L \) rounds, each round is characterized by the following eight steps (see figure 1):

(i) Every party (Alice\(_i\)) prepares an optical pulse \( a_i \) in an entangled state with a qubit \( A_i \), given by:

\[
|\psi\rangle_{A_i,a_i} = \sqrt{q} |0\rangle_{A_i} |0\rangle_{a_i} + \sqrt{1-q} |1\rangle_{A_i} |1\rangle_{a_i}, \quad \forall i \in \{1, 2, \ldots, N\},
\]

where \( 0 \leq q \leq 1 \), \( |0\rangle_{a_i} \) is the vacuum state, \( |1\rangle_{a_i} \) is the single-photon state, and \( \{|0\rangle_{A_i}, |1\rangle_{A_i}\} \) is the computational basis of qubit \( A_i \).

(ii) Every party sends her optical pulse \( a_i \) to the untrusted node via optical channels characterized by transmittance \( t \), in a synchronized manner.

(iii) The central node applies a Bell-multiport beam splitter [43–48] with \( M \) input and output ports\(^1\) to the incoming pulses and features a threshold detector \( D_i \) at each output port \( i = 1, \ldots, M \). The action of the multiport beam splitter is defined by the unitary transformation given in figure 1.

(iv) The central node announces the measurement outcome \( k_i \) for every detector \( D_i \) with \( k_i = 0 \) and \( k_i = 1 \) corresponding to a no-click and a click event, respectively. The round gets discarded if \( \sum_{i=1}^{M} k_i \neq 1 \), i.e. whenever single-photon interference did not occur in the central node. The probability that only detector \( D_j \) clicked is \( p_j \).

\(^1\) We assume that there are at least as many input ports of the beam splitter as parties taking part to the protocol, i.e. \( M \geq N \).
(v) According to a preshared secret key of $L \cdot h(p_{\text{PE}})$ bits\(^2\), the round is classified as a parameter-estimation (PE) round with probability $p_{\text{PE}}$ or as a key-generation (KG) round with probability $1 - p_{\text{PE}}$. There are on average $m = M p_{\text{PE}} L p_{\text{PE}}$ PE rounds that do not get discarded.

(a) In case of a PE round, every party measures her qubit in the $Z$-basis and then announces the measurement outcome to compute the frequency: $Q^m_{Z} = (1 + \langle Z^{\otimes N} \rangle_m) / 2$.

(b) In case of a KG round, conditioned on detector $D_j$ clicking, Alice$_i$ measures her qubit in the basis of the operator $O_{XY}(\varphi_i) = \cos \varphi_i X + \sin \varphi_i Y$ (where $X$ and $Y$ are the Pauli operators), with $\varphi_i = \arg(U_{ij})$ ($U_{ij}$ is given in figure 1). The parties announce $m$ randomly chosen measurement results in order to estimate the quantum bit error rate (QBER) by computing the frequency:

$$Q^m_{AA_{ij}} = (1 - \langle O_{XY}(\varphi_i)O_{XY}(\varphi_j) \rangle_m) / 2,$$

i.e. the frequency of discordant outcomes.

(vi) The secret key shared by the $N$ users is extracted from the remaining $n = M p_{\text{PE}} L - 2m$ raw key bits of the KG rounds.

(vii) Alice$_1$ broadcasts the error correction information that every other party uses to correct her raw key to Alice$_1$’s raw key.

(viii) Alice$_1$ broadcasts a suitable two-universal hash function and every party applies it to her key for privacy amplification.

Remarks. Note that the quantity $Q^m_{Z}$ is the frequency of the outcome +1 when the parties measure the operator $Z^{\otimes N}$. By making an analogy with the bipartite scenario, one can view $Q^m_{Z}$ as an estimation of the phase-error rate between Alice$_1$ and the other $N - 1$ parties (when the phase-error rate is defined as in [24]).

Since the Bell-multiport beam splitter redirects each incoming photon with equal probability to each potential output port, the probability of having a click in only one specific detector is the same for all detectors, i.e. $p_j$ reads the same for $j = 1, \ldots, M$. For this reason, the total probability of having exactly one click in any detector is given by $M p_j$.

In an honest implementation of the protocol, where the parties’ state preparation and the operations of the central node are carried out as described above, the state of the qubits $A_1, \ldots, A_N$ from which the parties distill a secret key is approximately a $W$-class state of $N$ qubits [42], as we show in section 2. Therefore, the protocol here introduced represents an alternative to other multipartite QKD protocols [34–38] where the entanglement resource used to generate the key is, instead, a noisy version of the GHZ state of $N$ qubits. Moreover, the $W$-class state used by the CKA is an entangled state which is post-selected after the interference of one single photon at the multiport beam splitter. Thus the resulting key rate scales linearly with the transmittance $t$ of one of the quantum channels linking the parties to the central node. This is in contrast to the other mentioned multipartite QKD protocols [34–38], where the distribution of an $N$-qubit GHZ state (e.g. encoded in orthogonal polarizations of a photon) would lead to a key rate which scales with $t^N$ (with $t$ being the transmittance of the link between one party and the node distributing the GHZ state). This makes our CKA much more suited to high-loss scenarios than previously proposed multipartite QKD protocols.

2. Multipartite QKD with a $W$ state

As mentioned at the end of section 1, the entanglement resource exploited to distill the secret key is a noisy $W$-class state of $N$ qubits [42], which is post-selected after single-photon interference occurred in the central node. In fact, the optimization of the CKA key rate (section 4) over the parameter $q$ weighting the initial superposition of the qubit-photon state always yields values of $q$ close to 1. This means that the quantum signal sent by the parties is strongly unbalanced towards the vacuum. Thus the events in which one of the detectors clicks are mainly caused by the arrival and detection of one photon. However, because of the balanced superposition generated by the multiport beam splitter, the detected photon could be sent by any party with equal probability. Since the photon is initially entangled to the qubit in state $|1\rangle$, the qubits’ state conditioned on the detection is a coherent superposition of states in which one qubit is in state $|1\rangle$ and all the others are in state $|0\rangle$, that is the mentioned $W$-class state. A secret conference key can then be extracted by proper measurements performed on such a state.

\(^2\) Where $h(x) = -x \log_2 x - (1 - x) \log_2 (1 - x)$ is the binary entropy function.
Let us start by considering the simplistic scenario in which the parties share the N-partite W state:

$$[W]_N = \frac{1}{\sqrt{N}} \left[ |00 \ldots 01\rangle + |00 \ldots 10\rangle + \ldots + |10 \ldots 00\rangle \right].$$

(2.1)

It has been proven [35] that the parties cannot extract perfectly correlated outcomes in any set of local measurement bases (for $N \geq 3$). Indeed, the only $N$-qubit state achieving that and yielding uniformly distributed random measurement outcomes is the GHZ state. Nevertheless, the $N$-partite W state can still be used to extract a secret conference key. The key bits are given by the outcomes of the $X$-basis measurements performed by the $N$ parties on their respective qubit. The expected QBER between any two parties is given by $1/2 - 1/N$, which amounts to subtracting the fraction $h(1/2 - 1/N)$ from the secret key rate due to error correction ($h(x)$ is the binary entropy). On the other hand, the eavesdropper’s knowledge about the key can be estimated via the phase-error rate $Q_x$ (as defined in section 1, more details in appendix A), which turns out to be zero on the W state. This is crucial for having a non-zero key rate even when the number of parties is large. The resulting asymptotic key rate, when the parties share an $N$-partite W state, is given by $1 - h(1/2 - 1/N)$.

Our CKA is constructed following the same philosophy. The only difference is that the conditional state shared by the parties after the detector’s click is not exactly the W state given by (2.1), but rather a noisy W-class state (the full expression is given in appendix B). Indeed, the multiport beam splitter introduces complex phases in the balanced superposition of states shared by the parties, that depend on which detector clicked. For this reason, we require the parties to adjust their KG measurements in the $X$, $Y$ plane in order to remove such phases and obtain the same QBER ($1/2 - 1/N$) they would observe by measuring in the $X$-basis had they shared the standard W state (2.1). However, the adjusted KG measurements do not commute with the operations performed in the untrusted node and prevent the CKA from being recast as an MDI prepare-and-measure scheme, opposed to its bipartite version [24]. Consequently, the multipartite scheme presented here is more challenging to implement than its bipartite counterpart, i.e. the TF-QKD protocol. In particular, it cannot be reformulated as a scheme where the parties prepare coherent states and send them to node $C$ for measurement. Nonetheless, the operations that the parties are required to perform seem to be within technological reach [49, 50]. In particular, the qubit system could be realized by a nitrogen-vacancy electron spin, whose coherence time has recently reached the order of seconds [51]. The entanglement between the electron spin and the photon’s Fock state would then be generated via selective optical pulses and coherent rotations [49], which would entangle the electron spin with the presence or absence of a photon.

3. Finite-key analysis

The protocol presented in section 1 can be effectively regarded as an $N$-partite QKD protocol solely characterized by the unknown quantum state $\rho_{\text{MP,LA}}$, which is the global state of the parties’ qubits in all the rounds that were not discarded. In this way we allow the eavesdropper, who is in total control of the untrusted node, to perform any kind of operation (coherent attacks) on the whole set of signals sent by the parties in the different rounds. As described above, in each round the parties perform trusted measurements on the state $\rho_{\text{MP,LA}}$, according to the preshared key they hold. The security of such a multipartite QKD protocol can be proven thanks to the finite-key analysis developed in [37]. In particular, since Alice$_i$ (who holds the key to which all the other parties correct their raw key) measures her qubit only in the two mutually unbiased bases $Z$ and $X$, the protocol’s security proof follows analogous lines to the one of the $N$-BB84 protocol presented in [37]. The security is guaranteed even when the state preparation and the measurement devices of the other parties (Alice$_2$, ..., Alice$_N$) are not trusted (a detailed proof is given in appendix A).

**Theorem 1.** The CKA in section 1, with the optimal 1-way error-correction protocol (which is $\varepsilon_{\text{EC}}$-fully secure and $2(N - 1)\varepsilon_{\text{PE}}$-robust) and where the secret key generated by two-universal hashing has length

$$\ell(N) = \left\lfloor \log_2 \left( 2( N - 1) \frac{1}{\varepsilon_{\text{EC}}} - 2 \log_2 \frac{1}{\varepsilon_{\text{PE}}} - 2 \log_2 \frac{1}{\varepsilon_{\text{PA}}} \right) \right\rfloor$$

(3.1)

is $\varepsilon_{\text{tot}}$-secure with $\varepsilon_{\text{tot}} = 2\varepsilon_{\text{PE}} + \varepsilon_{\text{EC}} + \varepsilon_{\text{PA}}$, where $\varepsilon_{\text{PE}}$ is defined as:

$$\varepsilon_{\text{PE}} \equiv \sqrt{(N - 1)\varepsilon_x + \varepsilon_z}$$

(3.2)

3 On average, the number of rounds that are not discarded by the CKA is $\text{MP,L}$. 

New J. Phys. 21 (2019) 123002
and \( \gamma(n, m, \Lambda_m, \varepsilon) \) is the positive root of the following equation:
\[
\ln \left( \frac{n(\Lambda_m + \gamma) + m\Lambda_m}{m\Lambda_m} \right) + \ln \left( \frac{(n + m)(1 - \Lambda_m) - n\gamma}{m(1 - \Lambda_m)} \right) = \ln \left( \frac{n + m}{m} \right) + \ln \varepsilon.
\]  
(3.3)

We remark that the length \( L \cdot h(p_{PE}) \) of the preshared key must be subtracted from the secret key length in order to have the net amount of fresh secret key bits. We also remark that our leakage estimation considers the worst-case QBER affecting the parties’ raw keys, which is (with high probability) not larger than the QBER observed in appositely designated KG rounds with the appropriate statistical correction. This is in contrast to several other finite-key analyses [52–55], where either the QBER is assumed to be known a priori or its estimation does not account for statistical fluctuations. In the asymptotic regime \( (L \to \infty) \), the finite-size effects are not present and the secret key rate \( r = \varepsilon/L \) reads:
\[
r(N) = M_p \left[ 1 - h(Q_Z) - \max_{i \in \{1, \ldots, N\}} h(Q_{A_iA_i}) \right],
\]  
(3.4)

where \( Q_Z \) and \( Q_{A_iA_i} \) are the probabilities correspondent to the frequencies defined in section 1.

4. Simulations

In this section we provide plots of the secret key rate—number of secret key bits per round—achieved by the CKA both with finite-key effects (3.1) and in the asymptotic regime (3.4), as a function of the loss in one of the channels linking a party to the central node, measured in dB \((-10 \log_{10} \ell)\). We assume that the protocol is honestly implemented as described in section 1 and we account for a dark count probability of \( p_{DC} = 10^{-9} \) in every detector (which can be attained with superconducting nanowire single photon detectors [29]) and for a polarization and a phase misalignment between Alice and each other party of 2\%. The relevant error rates and probabilities for this configuration are given in appendix B. The plots are optimized over the parameter \( g \) of the initial superposition between the two qubit–photon states, unless otherwise stated. The finite-key plots are further optimized over the probability \( p_{PE} \) of performing a PE round and over the security parameters \( \varepsilon_{xx}, \varepsilon_{xz}, \varepsilon_{EC} \) and \( \varepsilon_{PAB} \), constrained by a fixed total security parameter of \( \varepsilon_{tot} = 10^{-8} \).

In order to assess the performance of our CKA with an untrusted node, we consider the situation in which the central node is removed and the \( N \) parties are linked by a star network, where the transmittance of the link between any two parties is \( \ell^2 \). For this configuration, we consider the conference key rate generated by the following strategy and compare it to our CKA key rate. One selected party performs the best possible bipartite QKD scheme with every other party in the network, i.e. \( N - 1 \) times. Because of the network symmetry, every bipartite secret key has the same length and its asymptotic rate is upper bounded by the Pirandola–Laurenza–Ottaviani–Banchi bound [33] given by:
\[
\log_2 \left( 1 - \ell^2 \right).
\]  
Then, the selected party encodes the final conference key by using the keys she/he established singularly with each other party. Hence, the conference key length is equal to the bipartite keys’ lengths, but the total number of rounds \(^4\) needed to establish the conference key is given by the number of rounds performed by a pair of parties, multiplied by the number of bipartite schemes \( (N - 1) \).

Thus the conference key rate achieved by this strategy is upper bounded by:
\[
r_{\text{direct}}(N) = \frac{-\log_2 (1 - \ell^2)}{N - 1}.
\]  
(4.1)

We will refer to (4.1) as the direct-transmission bound, even though we emphasize that it only upper bounds the achievable conference key rate when the strategy we just described is employed. Indeed, we do not claim that this strategy yields the highest possible conference key rate for the considered network configuration. In this section we show that our CKA provides an advantage, in terms of performance, with respect to the above strategy (4.1).

4.1. Asymptotic regime

In figure 2 we plot the asymptotic key rate of the CKA (equation (3.4), solid and dotted lines) as a function of the loss in one of the quantum channels, for different number parties establishing the secret conference key. In particular, the solid lines are obtained by fixing \( M = N \), i.e. the number of input (output) ports of the beam splitter is given by the number of parties taking part to the protocol. The dotted lines are instead obtained by fixing the number of ports to \( M = 10 \). Finally, the dashed lines represent the direct-transmission bound (4.1) for the correspondent number of parties.

We observe that the CKA key rate can surpass the direct-transmission bound for sufficiently high losses. This is expected since the CKA key rate basically scales linearly with the transmittance \( \ell \) of the quantum channel.

\(^4\) By round we mean a set of steps of a given QKD protocol which contains only one transmission of quantum signals (more parties at the same time can transmit a quantum signal).
The QBER scales with the number of parties as linking one party to the central node, while the direct-transmission rate scales linearly with the transmittance allowed to use it in pairs protocols could be the following. The parties are given the same CKA experimental setup but they are now a detector, i.e. at high losses.

On the performance becomes tangible when their probability is comparable to the probability of having a click in counts of the whole channel linking two parties \[ N \] (black, blue, red and green; top to bottom). The CKA key rate overcomes the correspondent direct-transmission bound for increasing losses, as the number of parties increases. For instance, the CKA performed by 5 parties becomes advantageous at distances larger than 130 km (assuming a fiber attenuation of \[ \alpha = 0.2 \text{ dB km}^{-1} \]). We also observe that having more ports in the beam splitter than parties involved in the protocol is advantageous at low losses (dotted lines are above the solid lines) but disadvantageous at high losses, where more ports imply a higher chance of having a dark count.

\[ \text{Figure 2. The CKA key rate (equation (3.4), solid and dotted lines) and the direct-transmission bound (equation (4.1), dashed lines), as a function of the loss in the channel linking one party to the central node, for different number of parties } N = 2, 3, 5 \text{ and } 9 \text{ (black, blue, red and green; top to bottom). The CKA key rate overcomes the correspondent direct-transmission bound for increasing losses, as the number of parties increases. For instance, the CKA performed by } N = 5 \text{ parties becomes advantageous at distances larger than } 130 \text{ km (assuming a fiber attenuation of } \alpha = 0.2 \text{ dB km}^{-1} \text{). We also observe that having more ports in the beam splitter than parties involved in the protocol is advantageous at low losses (dotted lines are above the solid lines) but disadvantageous at high losses, where more ports imply a higher chance of having a dark count.} \]

From figure 2 we also deduce that performing the CKA with a higher number of ports in the beam splitter (dotted lines, where \( M = 10 \)) is advantageous at low losses and disadvantageous at high losses. The advantage of having more output ports is that the probability that two photons arrive at the same detector diminishes (this is an error source in our CKA). However, these errors could only occur if there is a non-negligible probability that two photons arrive at the central node, i.e. when the losses are low. At the same time, the presence of more output ports—and thus detectors—increases the chances of a dark count. And the negative effect of dark counts on the performance becomes tangible when their probability is comparable to the probability of having a click in a detector, i.e. at high losses.

Another relevant scenario for assessing the CKA performance in comparison to the iteration of bipartite protocols could be the following. The parties are given the same CKA experimental setup but they are now allowed to use it in pairs (or larger subgroups) in consecutive runs, effectively performing the original TF-QKD protocol [24]. Protocol 1 between one selected party and every other party. The different established keys are then used to encode the final conference key, similarly to the direct-transmission scenario. This strategy can then be compared to the case where the parties choose to use the CKA setup all at once, thus performing a truly multiparticle QKD scheme. A detailed analysis of this comparison in the asymptotic regime is given in appendix C. It turns out that, depending on the loss and on the state preparation, it is still advantageous to perform a multipartite protocol instead of iteratively executing bipartite protocols, on the CKA experimental setup.

4.2. Finite-key effects

In figure 3(a) we plot the finite-key conference rate (equation (3.1) divided by \( L \)) as a function of the number of rounds \( L \), for different fixed values of the loss (20 and 30 dB, solid and dotted–dashed lines) and different number of parties. We stress the fact that we normalize the key length to the total number of rounds \( L \), i.e. we

\[ \text{The QBER scales with the number of parties as } 1/2 - 1/N, \text{ see section 2.} \]
also take into account the rounds that get discarded due to double-clicks or no click in the detectors. The horizontal dashed lines correspond to the value of the direct-transmission bound (4.1) for the various combinations of losses and number of parties. We observe that the number of rounds leading to a non-zero key rate is in general higher than other multipartite schemes (see for example [37]). This is caused by the fact that the CKA devised here relies on single-photon interference events, which are only a fraction of all the events occurring in an experiment run. A considerable amount of rounds gets thus discarded, but still contributes to the rounds’ count. Nevertheless, the number of rounds needed for a non-zero key rate is comparable to other bipartite TF-QKD protocols [56, 57]. On the other hand, the advantage of relying on single-photon interference in a multipartite scenario is the excellent scaling of the protocol’s key rate with respect to losses, which allows it to overcome the asymptotic direct-transmission bound (dashed lines) even with a finite number of rounds.

In figure 3(b) we instead plot the minimum number of rounds \( L_{\text{min}} \) such that the finite-key rate \( \ell / L \) does not decrease more than 90% with respect to its asymptotic value \( r \) (3.4), i.e.: \( \ell / L_{\text{min}} \geq r / 10 \). The threshold \( L_{\text{min}} \) is plotted as a function of the number of parties \( N \) and for fixed values of the loss. We observe that \( L_{\text{min}} \) increases both with the number of parties and with the loss. The reason is that, in both cases, the fraction of the total number of rounds that gets discarded increases. This has a negative effect both on the asymptotic rate and on the finite-key rate, however the effect on the latter is greater, thus requiring a larger number of rounds \( L_{\text{min}} \) to maintain the finite-key rate within 90% range of the asymptotic one. Indeed, a larger fraction of discarded rounds decreases the prefactor \( M_{p} \) in both the finite- and the asymptotic-key rates, but it additionally decreases the number of rounds used for PE in the finite-key regime. This causes larger statistical fluctuations and thus a smaller finite-key rate.

5. Conclusions

In this work we introduced a new multipartite QKD protocol that exploits for the first time the correlations derived from an \( N \)-partite W state [42] to establish a secret conference key among the \( N \) users. In an honest implementation of the protocol, the \( W \) state is post-selected thanks to the interference of a single photon in a central node, extending the idea of the bipartite TF QKD protocol devised in [24] to the multipartite scenario. Hence the resulting key rate scales linearly with the transmittance of one of the quantum channels linking the parties to the central node, making the protocol particularly suited for conference keys established in high-loss scenarios.

We prove the protocol’s security in the finite-key regime by considering the most adversarial situation possible, i.e. coherent attacks are allowed by the eavesdropper. In order to achieve this, we rely on previous results on the finite-key security of multipartite QKD schemes derived in [37] and employ the entropic uncertainty relation [38].

![Figure 3. (a) Finite-key conference rate (equation (3.1) over \( L \)) as a function of the number of rounds \( L \) for fixed losses of 20 dB (solid lines) and 30 dB (dotted-dashed lines), and different number of parties: \( N = 2, 3 \) and 5 (black, blue and red; top to bottom). We observe that the rates quickly achieve their asymptotic value once the number of non-discarded rounds is enough to get a non-zero key. The CKA key rates overcome the direct-transmission bound (dashed lines) even in the finite-key scenario. (b) Minimum number of rounds such that the finite-key rate (equation (3.1) over \( L \)) is at least 10% of its asymptotic value, as a function of the number of parties and for fixed losses (1 dB blue circles, 20 dB red squares and 40 dB green diamonds).](image)
We provide simulations of the conference key rate both in the finite- and in the asymptotic-key regime. We compare the performance of our CKA to that achieved by performing bipartite QKD schemes between one party and each of the others and then using the established keys to encode the conference key. In particular, we analyze the cases where the bipartite schemes are performed with the same setup used for the CKA (in appendix C) and in the direct-transmission scenario (i.e. the central node is removed and the optimal bipartite QKD scheme is performed). We show that, in both cases, the execution of a truly multipartite scheme could be advantageous even when finite-key effects are accounted for.

Although the feasibility of the proposed CKA requires further investigation, with this work we demonstrate that, in principle, multipartite QKD does not necessarily need a GHZ-class state as its entanglement resource and that it can be implemented even in high-loss scenarios.

**Acknowledgments**

We thank Marcos Curty, Daniel Miller and Hua-Lei Yin for helpful discussions. This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 675662.

**Appendix A. Security proof**

In order to prove the security of our CKA in the finite-key scenario, we start from the general security statement given in [37, theorem 1]. The resulting secret key length is thus determined by the amount of information the eavesdropper has about the secret key and by the information the parties leak during the classical post-processing. The former is quantified by the min-entropy $H_{\min}^\epsilon(\rho_{XE}^m|E)$, where $\rho_{XE}^m$ is the classical–quantum state of Alice’s raw key and the eavesdropper’s quantum system $E$ which is partially correlated to it. Since the eavesdropper’s system is unknown, one cannot directly compute the mentioned min-entropy. Nevertheless, it can be bounded by means of the uncertainty relation [58] for smooth-entropies as follows:

$$H_{\min}^\epsilon(\rho_{XE}^m|E) \geq n - H_{\max}(\rho_{X_{m-1}Z_0}^m|Z_2...Z_N),$$  \hspace{1cm} (A.1)

where the max-entropy on the rhs quantifies the uncertainty of Alice’s Z-measurement results when the Z-outcomes of the remaining $N-1$ parties are known, if all parties would measure $Z$ in the $n$ rounds yielding the raw-key. The max-entropy can be upper bounded via the phase-error rate $Q^m_Z$ as defined in section 1—of the $n$ raw-key rounds. We get:

$$H_{\min}^\epsilon(\rho_{XE}^m|E) \geq n - n \cdot h(Q^m_Z),$$  \hspace{1cm} (A.2)

where $h(\cdot)$ is the binary entropy function: $h(x) = -x \log_2(x) - (1 - x) \log_2(1 - x)$. Finally, since the parties do not directly observe the phase-error rate $Q^m_Z$ of the $n$ rounds producing the raw key, this can be inferred through the theory of random sampling without replacement. In particular, the phase-error rate of the raw key $(Q^m_Z)$ can be upper bounded with high probability, once the observed phase-error rate $(Q^m_Z)$ is known. For this, we make use of the following tail inequality [56, lemma 1] which features a tighter bound with respect to the Serfling inequality.

**Lemma 1.** [56]. Let $X_{n+m}$ be a random binary string of $n + m$ bits, $X_m$ be a random sample (without replacement) of $m$ entries from the string $X_{n+m}$, and $X_n$ be the remaining bit string. Upon calling $\Lambda_m$ and $\Lambda_n$ the frequencies of bit value 1 in string $X_m$ and $X_n$, respectively, for any $\varepsilon > 0$ it holds:

$$\Pr[\Lambda_n \leq \Lambda_m + \gamma(n, m, \Lambda_m, \varepsilon)] > 1 - \varepsilon,$$  \hspace{1cm} (A.3)

where $\gamma(n, m, \Lambda_m, \varepsilon)$ is the positive root of the following equation:

$$\ln\left(\frac{n(\Lambda_m + \gamma) + m\Lambda_m}{m\Lambda_m}\right) + \ln\left(\frac{(n + m)(1 - \Lambda_m) - n\gamma}{m(1 - \Lambda_m)}\right) = \ln\left(\frac{n + m}{m}\right) + \ln\varepsilon.$$  \hspace{1cm} (A.4)

By applying lemma 1 to the case of $Q^m_Z$, we can finally bound the eavesdropper knowledge about the secret key as follows:

$$H_{\min}^\epsilon(\rho_{XE}^m|E) \geq n - n \cdot h(Q^m_Z + \gamma(n, m, Q^m_Z, \varepsilon)).$$  \hspace{1cm} (A.5)

The remaining part of the secret key length that needs to be estimated is the error-correction information sent through the classical public channel, and thus leaked to the eavesdropper. Since we consider a one-way scheme where Alice broadcasts the same error-correction information to all the parties through the public channel, the information gained by the eavesdropper is bounded by the binary entropy of the worst QBER between Alice and any other party, by means of [37, theorem 2].
Putting these considerations together, we obtain the security statement given in theorem 1.

We remark that the only requirements needed for the security proof to hold are that Alice$_1$ is actually measuring qubits and that her measurement device is working as expected (i.e. it measures in the \(X\) and \(Z\) basis) [58, 59]. This means that we do not need to trust the measurement devices of the other parties (as long as they are memoryless), nor their state preparation (including Alice$_1$’s).

### Appendix B. Channel model

In this section we compute the QBER \((Q_{AA})\), the phase-error rate \((Q_{\phi})\) and the probability that a given detector clicked \(p_d\), assuming that the protocol is implemented as described in section 1. We also account for a dark count probability \(p_d\) in each detector and we consider the specific scenario in which there are a polarization and a phase misalignment of angles \(\theta\) and \(\phi\), respectively, between Alice$_1$ and each other party. In the simulations of section 4 we set \(p_d = 10^{-9}\) and \(\phi = \arcsin(0.02)\). For simplicity, we assume that the input signals of the \(N\) parties enter the first \(N\) ports of the \(M\)-port beam splitter. Nevertheless, the results in terms of achieved key rate are independent of which input ports are used, thanks to the balanced redistribution of the input photons to the output ports of the considered Bell-multiport beam splitter (see figure 1). We remark that the expressions derived here together with the asymptotic key rate given in (3.4) reproduce those of the original TF-QKD protocol [24, Protocol 1] in the case of two parties \((N = 2)\) with a balanced 2-port beam splitter \((M = 2)\).

We first derive the QBER, the phase-error rate and the probability \(p_d\), assuming no dark counts in the detectors, i.e. every click is caused by the arrival of one or more photons. In the last Subsection we use the derived expressions to obtain analogous quantities, with the assumption that every detector has a probability \(p_d\) of clicking conditioned on no photon arriving.

#### B.1. Qubits’ state conditioned on one click

According to the protocol, the global state of the parties’ qubits and signals, before sending the signals to the central node, reads:

\[
|\Phi_1\rangle = \bigotimes_{k=1}^N |\phi\rangle_{Ak}a_k = \bigotimes_{k=1}^N (\sqrt{q} |0\rangle_{Ak} |0\rangle_{ak} + \sqrt{1-q} e^{i\phi} |1\rangle_{Ak} a_k^2 |0\rangle_{ak}),
\]

where the phase mismatch \(\phi_k\) is defined as zero if \(k = 1\) and as \(\phi\) if \(k = 1,\ldots, N-1\), which means that every other party has the same phase mismatch with respect to Alice$_1$. The signals \(a_k\) are then sent to the central node through lossy optical channels, which are modeled as beam splitters with transmittance \(t\). The global state after the transmission of the signals to the untrusted relay reads:

\[
|\Phi_2\rangle = \bigotimes_{k=1}^N (\sqrt{q} |0\rangle_{Ak} (1 - q^{1/2} e^{i\phi} |1\rangle_{Ak} a_k^2 + \sqrt{1-t} l_k^1) |0\rangle)
\]

where \(l_k^1\) is the creation operator of the lost photon in channel \(k\), \(\bar{b}\) is a \(N\)-bit vector that runs from 0 to \(2^N - 1\) in binary notation (covering all the possible combinations of qubit states) and \(|\bar{b}\rangle\) is the Hamming weight of vector \(\bar{b}\). From now on, we denote as \(g(\cdot)\) the bijective function that takes as input a binary vector and outputs the correspondent decimal number.

We assume now that the polarization of the photons sent by Alice$_2$, … Alice$_N$ is rotated by an angle \(\theta\) with respect to Alice$_1$’s signal:

\[
|\Phi_3\rangle = \bigotimes_{k=1}^{N-1} q^{-g(\bar{b})/2} (1 - q^{1/2} e^{i\phi} |1\rangle_{Ak} a_k^2 - \sqrt{1-t} l_k^1) |0\rangle e^{i\theta_k a_k^2 P_k} - \sqrt{1-t} l_k^1 |0\rangle e^{i\theta_k a_k^2 P_k} + \sqrt{1-t} l_k^1 |0\rangle e^{i\theta_k a_k^2 P_k},
\]

where \(\theta_k\) is defined as zero if \(k = 1\) and as \(\theta\) if \(k = 1,\ldots, N-1\), while the subscripts \(P_k\) and \(P_k\) indicate the polarization of Alice$_1$’s signal and its orthogonal direction, respectively.

Finally, the global state after the application of the Bell-multiport beam splitter on the incoming signals (its action on the incoming creation operators is reported in figure 1) is:
where we expanded the product in the second line whenever \( g(\vec{b}) = 0 \), since it would correspond to a vacuum state for the outcome signal \( j \). We now focus on rewriting the following term:

\[
|\psi\rangle_{\sigma_j} = \prod_{k=1}^{N} e^{i\theta_k} |\sqrt{\mathcal{U}_j} (\cos \theta_k \sigma_j^{1,\vec{p}} - \sin \theta_k \sigma_j^{1,\vec{p}}) + \sqrt{1 - t} l_k^j \rangle_{d_k^j} |0\rangle
\]

(\text{B.7})

where we expanded the product in the first line of (B.7) by introducing a sum over the binary vector \( \vec{d} \). The sum runs over all the \( N \)-bit vectors \( \vec{d} \) for which \( d_k = 0 \) whenever \( b_k = 0 \), for all \( k \) – the condition \( d_k \land b_k = d_k \forall k \). This is to make sure that the \( k \)-th factor in the first line does not contribute to the expanded product in the second line whenever \( b_k = 0 \). The remaining bits of \( \vec{d} \) that are not affected by the mentioned condition, can be either 1 or 0. If \( d_k = 1 \) we intend that, for this particular term in the sum, the contribution of the \( k \)-th factor in the first line of (B.7) is given by its first addend (\( \sqrt{\mathcal{U}_j} (\ldots) \)). While if \( d_k = 0 \) and \( b_k = 1 \), we mean that the contribution is coming from the second addend (\( \sqrt{1 - t} l_k^j \)). The exponents in the second line of (B.7) are chosen according to these rules. Finally, (B.8) is obtained by using the definition of \( \mathcal{U}_j \) from figure 1 and by applying the creation operators on the vacuum. We now expand the remaining product in (B.8) with the same technique and obtain the following expression:
We use the Kronecker deltas to reduce the sums over 
By substituting 
We now substitute 
Putting everything together allows to simplify 
Finally, the 
Finally the 

We now substitute (B.9) back into (B.6) and note that the effect of the projectors \((\text{id}_{\gamma} - P_{(0)}_{\gamma}) \otimes_{i \neq j} P_{(0)}_{\gamma}\) is to remove the case \(g(\tilde{d}) = 0\) from (B.9). Hence we get:

\[
(\text{id}_{\gamma} - P_{(0)}_{\gamma}) \otimes_{i \neq j} P_{(0)}_{\gamma}|\psi\rangle = e^{i \delta_{\gamma} \tilde{d}} (1 - q) e^{i \delta_{\gamma} \tilde{d}} |\psi\rangle = e^{i \delta_{\gamma} \tilde{d}} (1 - q) e^{i \delta_{\gamma} \tilde{d}} |\psi\rangle.
\]

By substituting (B.10) into (B.5) we finally get the state of the qubits conditioned on \(D_i\) clicking:

\[
P_j \rho_{A_1 \ldots A_N} = \sum_{g(\tilde{d})=1}^{2^{N-1}} q^{N-|\tilde{d}|} e^{i \delta_{\gamma} \tilde{d}} (1 - q) e^{i \delta_{\gamma} \tilde{d}} |\psi\rangle \langle \psi| \rho_{A_1 \ldots A_N} |\psi\rangle.
\]

We use the Kronecker deltas to reduce the sums over \(\tilde{d}, \tilde{d}', \tilde{f}\) and \(\tilde{f}'\). The third delta fixes the value of \(\tilde{d}':\n\tilde{d}' = \tilde{b}' \oplus \tilde{d}' \oplus \tilde{d}.\) The fixed value of \(\tilde{d}'\) combined with the other constraints on this vector imply additional constraints on \(\tilde{d}.\) In particular, \(\tilde{d}' = 0\) implies \(\tilde{d} = \tilde{b}' \oplus \tilde{d}'\) while \(\tilde{d}' \wedge \tilde{d}' = \tilde{d}\) implies \(\tilde{b}' \wedge (\tilde{b} \oplus \tilde{d}) = \tilde{b}' \oplus \tilde{d}.\) Finally the first two deltas imply \(|\tilde{d}| = |\tilde{d}'|\), which combined with the third delta yields \(|\tilde{d}| = |b|\).

Putting everything together allows to simplify (B.11) as follows:

\[
P_j \rho_{A_1 \ldots A_N} = \sum_{g(\tilde{d})=1}^{2^{N-1}} q^{N-|\tilde{d}|} e^{i \delta_{\gamma} \tilde{d}} (1 - q) e^{i \delta_{\gamma} \tilde{d}} |\psi\rangle \langle \psi| \rho_{A_1 \ldots A_N} |\psi\rangle.
\]
where the sets of binary vectors \( \mathcal{D}(\vec{b}, \vec{b}') \), \( \mathcal{F}(\vec{d}) \) and \( \mathcal{F}'(\vec{f}, \vec{d}, \vec{b}, \vec{b}') \) are defined as follows:

\[
\mathcal{D}(\vec{b}, \vec{b}') = \{ \vec{d} \in g^{-1}\{(1, 2N - 1)\}: \vec{d} \wedge \vec{b} = \vec{d}, \ \vec{d} = \vec{b} \oplus \vec{b}', (\vec{b} \oplus \vec{d}) \wedge \vec{b}' = \vec{b} \oplus \vec{d} \} \hspace{1cm} (B.13)
\]

\[
\mathcal{F}(\vec{d}) = \{ \vec{f}' \in g^{-1}\{\{0, 2N - 1\}\}: \vec{f}' \wedge \vec{d} = \vec{f}', \ \vec{f}' = d_i \} \hspace{1cm} (B.14)
\]

\[
\mathcal{F}'(\vec{f}', \vec{d}, \vec{b}, \vec{b}') = \{ \vec{f}' \in g^{-1}\{\{0, 2N - 1\}\}: \vec{f}' \wedge (\vec{b} \oplus \vec{d} \oplus \vec{b}') = \vec{f}', \ \vec{f}' = b_i \oplus d_i \oplus b'_i, \ |\vec{f}'| = |\vec{f}'| \}. \hspace{1cm} (B.15)
\]

We can now sum over the vectors \( \vec{f}' \) since no term depends on them in \( (B.12) \):

\[
p_j \rho_{A_1 \ldots A_N}^{j} = \sum_{g(\vec{b}, \vec{b}' \in \mathcal{D}(\vec{b}, \vec{b}')) = 1} 2^{N-1} q^{N-|\vec{b}|} (1 - q)^{|\vec{b}|} \langle \hat{b} | e^{i(\theta' - \theta)} \hat{b} } \langle \hat{b}' | \rangle \langle \hat{b}' | \hat{b} \rangle \langle \hat{b} | \rangle
\]

\[
\times \sum_{\vec{d} \in \mathcal{D}(\vec{b}, \vec{b}')} e^{i \frac{\pi}{4} (j - 1) \sum_{k=1}^{N} (k - 1)d_k - h_k \oplus d_k \oplus b'_k) \left( \frac{t}{M} \right)^{|\vec{d}|} (1 - \tau)^{|\vec{b}| - |\vec{d}|}
\]

\[
\times 2^{N-1} \left( |\vec{b} \oplus \vec{d} \oplus \vec{b}'| - b_i \oplus d_i \oplus b'_i \right)^{|\vec{f}'|} (|\vec{d}|-|\vec{f}'|)! (\cos \theta)^{2|\vec{d}| - d_i - d_i \oplus b_i} (\sin \theta)^{2|\vec{d}| - |\vec{f}'|}. \hspace{1cm} (B.16)
\]

where the asterisk on the binomial coefficient means that it is defined as zero if \( |\vec{f}'| = 0 \) and \( b_i \oplus d_i \oplus b'_i = 1 \).

Finally, since every term just depends on \( |\vec{f}'| \), we can sum over all the vectors \( \vec{f} \) with equal Hamming weight and obtain the final expression for the conditional state of the qubits when detector \( D_j \) clicked:

\[
p_j \rho_{A_1 \ldots A_N}^{j} = \sum_{\vec{b}} 2^{N-1} q^{N-|\vec{b}|} (1 - q)^{|\vec{b}|} \langle \hat{b} | e^{i(\theta' - \theta)} \hat{b} } \langle \hat{b}' | \rangle \langle \hat{b}' | \hat{b} \rangle \langle \hat{b} | \rangle
\]

\[
\times \sum_{\vec{d} \in \mathcal{D}(\vec{b}, \vec{b}')} e^{i \frac{\pi}{4} (j - 1) \sum_{k=1}^{N} (k - 1)d_k - h_k \oplus d_k \oplus b'_k) \left( \frac{t}{M} \right)^{|\vec{d}|} (1 - \tau)^{|\vec{b}| - |\vec{d}|}
\]

\[
\times \left( |\vec{d}|-d_i \right)^{|\vec{f}'|} (|\vec{d}|-|\vec{f}'|)! (\cos \theta)^{2m - d_i - d_i \oplus b_i} (\sin \theta)^{2|\vec{d}| - |\vec{f}'|}. \hspace{1cm} (B.17)
\]

### B.2. Probability of exactly one click

We can now compute the probability \( p_j \) of having just one click in detector \( D_j \) by simply computing the trace of both sides in \( (B.17) \):

\[
p_j = \sum_{\vec{b}} 2^{N-1} q^{N-|\vec{b}|} (1 - q)^{|\vec{b}|} \sum_{\vec{d} \in \mathcal{D}(\vec{b}, \vec{b}')} e^{i \frac{\pi}{4} (j - 1) \sum_{k=1}^{N} (k - 1)d_k - h_k \oplus d_k \oplus b'_k) \left( \frac{t}{M} \right)^{|\vec{d}|} (1 - \tau)^{|\vec{b}| - |\vec{d}|}
\]

\[
\times \left( |\vec{d}|-d_i \right)^{|\vec{f}'|} (|\vec{d}|-|\vec{f}'|)! (\cos \theta)^{2m - d_i - d_i \oplus b_i} (\sin \theta)^{2|\vec{d}| - |\vec{f}'|}. \hspace{1cm} (B.18)
\]

In order to obtain an easier expression to compute, we distinguish the cases: \( b_1 = 0 \), \( b_1 = 1 \) and the special case \( \vec{b} = 100 \ldots 0 \):
By employing the following identity:

\[ p_j = \sum_{g(b) = 2}^{2^{N-1}} q^{N-|\vec{\beta}|}(1 - q)^{|\vec{\beta}|} \sum_{g(\vec{d}) = 2, d \perp \vec{d} \perp \vec{d}}^{2^{N-1}} \left( \frac{t}{M} \right)^{|\vec{d}|} (1 - t)^{|\vec{\beta}| - |\vec{d}|} \]

\[ \times \sum_{m=0}^{|\vec{d}|} \left( \frac{|\vec{d}|}{m} \right)^2 m!(|\vec{d}| - m)!(\cos \theta)^{2m}(\sin \theta)^{2(|\vec{d}| - m)} \]

\[ + q^{N-1}(1 - q) \left( \frac{t}{M} \right)^{|\vec{d}|} \quad \text{(this term comes from: } \vec{b} = 100 \ldots 0, \vec{d} = 100 \ldots 0) \]

\[ + \sum_{g(b) = 3}^{2^{N-1}} q^{N-|\vec{\beta}|}(1 - q)^{|\vec{\beta}|} \]

\[ \times \left[ \sum_{g(\vec{d}) = 2, d \perp \vec{d} \perp \vec{d}}^{2^{N-1}} \left( \frac{t}{M} \right)^{|\vec{d}|} (1 - t)^{|\vec{\beta}| - |\vec{d}|} \sum_{m=1}^{|\vec{d}|} \left( \frac{|\vec{d}|}{m} \right)^2 m!(|\vec{d}| - m)!(\cos \theta)^{2m-1}(\sin \theta)^{2(|\vec{d}| - m)} \right] \]

We can now partially sum over the vectors \( \vec{d} \) since the terms in the sums only depend on the Hamming weight of these vectors:

\[ p_j = \sum_{g(b) = 2}^{2^{N-1}} q^{N-|\vec{\beta}|}(1 - q)^{|\vec{\beta}|} \sum_{|\vec{d}| = 1}^{2^{N-1}} \left( \frac{|\vec{d}|}{|\vec{d}|} \right)^2 m!(|\vec{d}| - m)!(\cos \theta)^{2m}(\sin \theta)^{2(|\vec{d}| - m)} \]

\[ + q^{N-1}(1 - q) \left( \frac{t}{M} \right)^{|\vec{d}|} \]

\[ + \sum_{g(b) = 3}^{2^{N-1}} q^{N-|\vec{\beta}|}(1 - q)^{|\vec{\beta}|} \]

\[ \times \left[ \sum_{|\vec{d}| = 1}^{2^{N-1}} \left( \frac{|\vec{d}|}{|\vec{d}|} \right)^2 m!(|\vec{d}| - m)!(\cos \theta)^{2m}(\sin \theta)^{2(|\vec{d}| - m)} \right] \]

By employing the following identity:

\[ \sum_{m=0}^{|\vec{d}|} \left( \frac{|\vec{d}|}{m} \right)^2 m!(|\vec{d}| - m)!(\cos \theta)^{2m}(\sin \theta)^{2(|\vec{d}| - m)} = |\vec{d}|!(\cos \theta)^{2m}(\sin \theta)^{2(|\vec{d}| - m)} \]

\[ = |\vec{d}|!(\sin^2 \theta + \cos^2 \theta)^{|\vec{d}|} = |\vec{d}|! \]

both in the second and last row of (B.20), we get the following expression:

\[ p_j = \sum_{g(b) = 2}^{2^{N-1}} q^{N-|\vec{\beta}|}(1 - q)^{|\vec{\beta}|} \sum_{l=1}^{|\vec{\beta}|} \left( \frac{l}{M} \right)^{|\vec{\beta}| - |\vec{\beta}|} (1 - q)^{|\vec{\beta}| - |\vec{\beta}|} \]

\[ \times \sum_{m=0}^{|\vec{\beta}| - l} \left( \frac{|\vec{\beta}| - l}{m} \right)^2 m!(|\vec{\beta}| - m)!(\cos \theta)^{2m}(\sin \theta)^{2(|\vec{\beta}| - m)} \]

\[ + \sum_{l=1}^{|\vec{\beta}| - 1} \left( \frac{|\vec{\beta}| - l}{l} \right)^{|\vec{\beta}| - l - 1} (1 - q)^{|\vec{\beta}| - l - 1} \]

\[ \times \left[ \sum_{m=0}^{|\vec{\beta}| - l} \left( \frac{|\vec{\beta}| - l}{m} \right)^2 m!(|\vec{\beta}| - m)!(\cos \theta)^{2m}(\sin \theta)^{2(|\vec{\beta}| - m)} \right] \]

\[ + \sum_{l=1}^{|\vec{\beta}| - 1} \left( \frac{|\vec{\beta}| - l}{l} \right)^{|\vec{\beta}| - l - 1} (1 - q)^{|\vec{\beta}| - l - 1} \]

\[ \times \left[ \sum_{m=0}^{|\vec{\beta}| - l} \left( \frac{|\vec{\beta}| - l}{m} \right)^2 m!(|\vec{\beta}| - m)!(\cos \theta)^{2m}(\sin \theta)^{2(|\vec{\beta}| - m)} \right] \]
The remaining sum over \( m \) can be similarly simplified as follows:

\[
\sum_{m=0}^{l} \left( \frac{1}{m} \right)^{2} (m + 1)(l - m)!(\cos \theta)^{2m} (\sin \theta)^{2(l-m)} = l!(1 + l \cos^{2} \theta). \tag{B.23}
\]

By substituting (B.23) into (B.22) and by partially summing over vectors \( \tilde{b}' \) we obtain the final expression for the probability that only detector \( D_{l} \) clicks:

\[
p_{j} = Nq^{N-1}(1 - q)\left(\frac{t}{M}\right) + \sum_{r=2}^{N} \frac{1}{r!} \left[ \frac{N - 1}{r} \right] q^{N-r}(1 - q)^{r} \sum_{l=1}^{r} \left( \frac{t}{M} \right)^{l} (1 - t)^{r-l} \]

\[
+ \sum_{r=1}^{N} \frac{1}{r!} \left[ \frac{N - 1}{r} \right] q^{N-r}(1 - q)^{r} \sum_{l=1}^{r} \left( \frac{t}{M} \right)^{l} (1 - t)^{r-l} (l - 1)!(\sin^{2} \theta + l \cos^{2} \theta)
\]

\[+ \sum_{l=1}^{r} \left( \frac{t}{M} \right)^{l} (1 - t)^{r-l} \]. \tag{B.24}

We observe that the probability \( p_{j} \) that only detector \( D_{j} \) clicks is independent of the particular detector because of the symmetric action of the multiport beam splitter.

### B.3. QBER

Starting from the conditional state (B.17), we can compute the QBER between Alice_{1} and Alice_{k}'s outcomes when they measure their qubit in the eigenbasis of the operator \( O_{XY}(\varphi) \) and \( O_{XY}(\varphi_{k}) \), respectively, with \( O_{XY}(\varphi) = \cos(\varphi)X + \sin(\varphi)Y \) (\( X \) and \( Y \) are the Pauli operators). The operator \( O_{XY}(\varphi) \) has eigenvalues \( \lambda = \pm 1 \) and correspondent eigenvectors \( :|\lambda\rangle_{\varphi} = \frac{1}{\sqrt{2}}(|0\rangle + \lambda e^{i\varphi}|1\rangle) \).

To start with, we compute the following quantity:

\[
\langle \tilde{b}' | P_{A_{1}1}^{A_{1}} \otimes P_{|1-1\rangle A_{k}}^{A_{k}} | \tilde{b}' \rangle = \frac{1}{4} (e^{b_{i}i\varphi})((-1)^{N}e^{b_{i}i\varphi}) (e^{-b_{i}i\varphi})((-1)^{N}e^{-b_{i}i\varphi}) \prod_{l=1}^{N-k} \delta_{b_{l}b_{l}'} \tag{B.25}
\]

and we insert it into the probability that Alice_{1} measured the outcome +1 and Alice_{k} measured the outcome −1, when \( D_{l} \) clicked:

\[
\text{Tr}\left[ P_{A_{1}1}^{A_{1}} \otimes P_{|1-1\rangle A_{k}}^{A_{k}} \rho_{A_{1}...A_{N}} \right] = \frac{1}{4} \sum_{j=0}^{2N-1} \sum_{b' \in Q(\tilde{b}') \in Q(\tilde{b})} \left( (-1)^{b_{j} + b_{j}'} \frac{e^{2\pi i (j-1)(b_{j} - 1) - b_{j} + b_{j}'(e^{i\varphi} - e^{-i\varphi})}}{M^{j} (1 - t)^{j}} \right) \]

\[
\times \sum_{\tilde{d} \in Q(\tilde{b})} \left( \frac{\tilde{d}}{M} \right) (1 - t)^{j-1} \frac{2^{j} e^{2\pi i (j-1)(d_{j} - 1) - d_{j} + b_{j}'(e^{i\varphi} - e^{-i\varphi})}}{M^{j} (1 - t)^{j}}
\]

\[
\times \sum_{m=0}^{j} \frac{m}{m - d_{j}} \left( \frac{|\tilde{d} - d_{j}|}{m - d_{j}} \right) \left( \frac{|\tilde{d} + \tilde{d}' + \tilde{b}'|}{m - b_{j} + d_{j} + b_{j}'} \right)^{m} m!(|\tilde{d} - m|)! (\cos \theta)^{2m - d_{j} + b_{j}'(e^{i\varphi} - e^{-i\varphi}) (\sin \theta)^{2(|\tilde{d} - m|)}} \tag{B.26}
\]

where \( Q(\tilde{b}') \) is a set of at most 2 binary vectors, defined as: \( Q(\tilde{b}') = \{ \tilde{b}', \tilde{b}_{1} \tilde{b}_{2} ... \tilde{b}_{k} \} \) (iff \( \tilde{b}_{1} \oplus \tilde{b}_{k} = 1 \)).\(^{6}\) This means that the sum over \( \tilde{b}' \) is reduced to just one term, namely \( \tilde{b}' = \tilde{b} \), plus the possibility of a second term in which \( \tilde{b}' \) differs from \( \tilde{b} \) in position 1 and \( k \), as long as the bits of vector \( \tilde{b} \) differ from each other in those positions. Now we compute the sum over \( \tilde{b}' \) as follows:

\(^{6}\) The straight line over a bit indicates its negation.
we minimize the QBER and thus increase the secret key rate. This requires Alice

Finally, we split the sums over outcome +1 and obtains an identical expression to (B.29). In conclusion, the QBER conditioned on Dj clicking is given by twice the probability given in (B.29).

By fixing the angles \( \varphi_1 \) and \( \varphi_2 \) as mentioned in the protocol’s description: \( \varphi_1 = 0 \) and \( \varphi_2 = \arg(U_{\varphi_2}) = \frac{2\pi}{M}(k - 1)(j - 1) \) we minimize the QBER and thus increase the secret key rate. This requires Alice to adjust her measurement depending on which detector clicked, implying that such measurement does not commute with the operations performed by node C. On the other hand, the QBER is now minimal and reads the same regardless of which couple \((A_1, A_2)\) one considers or which detector \(D_j\) clicks.
\[ Q_{A_iA_k} = 1 - \frac{1}{2} p_j \cos \phi \cos \theta \sum_{r=0}^{N-2} \binom{N-2}{r} q^{N-2-r}(1 - q)^{r+1} \sum_{l=0}^{r} \binom{r}{l} (1 + 1)(\frac{t}{M})^{l+1} (1 - t)^{r-l}, \]  

(B.30)

where \( p_j \) is given in (B.24).

### B.4. Phase-error rate

Finally we compute the phase-error rate, defined as the probability that the product of the Z-measurement results of all the parties equals +1 (i.e. the qubit of an even number of parties collapsed in state \( |1 \rangle \)), which corresponds to the outcome \( Z = -1 \):

\[
Q_Z = \Pr\left[ \prod_{k=1}^{N} Z_{A_k} = 1 \right] = \text{Tr}\left[ \sum_{g(\tilde{f})=4}^{2^{N-1}} \sum_{l=1}^{r} \binom{r}{l} (1 - t)^{2r-l}! \rho_{A_1, \ldots, A_N} \right], \quad (B.31)
\]

where the quantum state \( \rho_{A_1, \ldots, A_N} \) conditioned on detector \( D \), clicking is given in (B.17) and the case \( g(\tilde{f}) = 0 \) is excluded since \( |0 \rangle \) does not appear in (B.17). By following analogous steps to those presented in appendix B.2 we obtain the following expression for the phase-error rate:

\[
Q_Z = \frac{1}{p_j} \sum_{r=1}^{\frac{N-1}{2r}} \binom{N-1}{2r} q^{N-2r}(1 - q)^{2r} \frac{2r}{l} \left( \frac{t}{M} \right)^{l}(1 - t)^{2r-l}! \\
+ \frac{1}{p_j} \sum_{r=1}^{\frac{N-1}{2r}} \binom{N-1}{2r} q^{N-2r}(1 - q)^{2r} \frac{2r-1}{l} \left( \frac{t}{M} \right)^{l}(1 - t)^{2r-l}! \\
+ \frac{2r}{l} \left( \frac{t}{M} \right)^{l}(1 - t)^{2r-l}(l - 1)! (\sin^2 \theta + l \cos^2 \theta). \quad (B.32)
\]

### B.5. Dark counts

So far we computed the quantities \( p_j, Q_{A_iA_k} \) and \( Q_Z \) assuming that every click in the detectors is due to the arrival of one or more photons. By naming \( \Omega_{ph} \) the event in which one or more photons arrive at detector \( D_i \) and no other photon arrives at any other detector, we can formally express the computed quantities as:

\[
p_j = \Pr(\Omega_{ph}), \quad (B.33)
\]

\[
Q_{A_iA_k} = \Pr(A_i \neq A_k|\Omega_{ph}), \quad (B.34)
\]

\[
Q_Z = \Pr\left[ \prod_{k=1}^{N} Z_{A_k} = 1 | \Omega_{ph} \right]. \quad (B.35)
\]

For the setup presented in section 1 and the channel model described at the beginning of this section, the explicit expressions of (B.33), (B.34) and (B.35) are given in (B.24), (B.30) and (B.32), respectively.

We now assume that every detector is characterized by a probability \( p_j \) of clicking conditioned on no photon arriving. We also define \( \Omega_{click} \) to be the event in which only detector \( D_i \) clicks and \( \Omega_{no\,ph} \) to be the event in which no photon arrives at any detector. Then, the error rates \( Q_{A_iA_k}^{dc} \) and \( Q_Z^{dc} \) and the probability \( p_j^{dc} \) that enter the key rate formula and that model the correspondent observed quantities read as follows:

\[
p_j^{dc} = \Pr(\Omega_{click}) = p_j(1 - p_j)^{M-1} + p_d(1 - p_d)^{M-1}\Pr(\Omega_{no\,ph}) \quad (B.36)
\]

\[
Q_{A_iA_k}^{dc} = \Pr(A_i \neq A_k|\Omega_{click}) \\
= \frac{1}{p_j^{dc}} [\Pr(A_i \neq A_k|\Omega_{no\,ph})\Pr(\Omega_{no\,ph})p_d(1 - p_d)^{M-1} + Q_{A_iA_k} p_j(1 - p_d)^{M-1}] \quad (B.37)
\]

\[
Q_Z^{dc} = \Pr\left[ \prod_{k=1}^{N} Z_{A_k} = 1 | \Omega_{click} \right] \\
= \frac{1}{p_j^{dc}} [\Pr\left( \prod_{k=1}^{N} Z_{A_k} = 1 | \Omega_{no\,ph} \right)\Pr(\Omega_{no\,ph})p_d(1 - p_d)^{M-1} + Q_Z p_j(1 - p_d)^{M-1}], \quad (B.38)
\]

where \( p_j, Q_{A_iA_k} \) and \( Q_Z \) are defined in (B.33), (B.34) and (B.35), respectively, while the probabilities related to the arrival of no photon read:
 protocols. In other words, it might be possible to outperform the multipartite CKA by iteratively executing its 
the CKA experimental setup and uses it to perform bipartite QKD 
Although we have shown in section 4 that a truly multipartite QKD scheme can outperform the iterative use of 
Appendix C. Optimized CKA

The probabilities (B.39), (B.40) and (B.41) are obtained by following similar steps to those presented in this 
section and that led to the final expressions for $P_j$, $Q_{AA}$, and $Q_{Zr}$, respectively. The starting point in this case is 
the conditional state of the qubits when no photon arrived at any detector:

$$
Pr(\Omega_{no\ ph}) = (q + (1 - q)(1 - t))^N
$$

$$
Pr(A_i = A_k | \Omega_{no\ ph}) = \frac{1}{2}
$$

$$
Pr\left(\prod_{k=1}^{N} Z_{A_k} = 1 | \Omega_{no\ ph}\right) = \frac{1}{Pr(\Omega_{no\ ph})} \sum_{l=0}^{\left\lfloor \frac{N}{2} \right\rfloor} \left(\begin{array}{c}
N - 2l \\
2l
\end{array}\right) q^{N-2l}(1-q)2l(1-t)2l.
$$

Appendix C. Optimized CKA

Although we have shown in section 4 that a truly multiparty QKD scheme can outperform the iterative use of
any bipartite QKD scheme in the direct-transmission scenario (i.e. the central node is removed), this does not 
necessarily hold when one has at hand the CKA experimental setup and uses it to perform bipartite QKD
protocols. In other words, it might be possible to outperform the multipartite CKA by iteratively executing its 
its bipartite version (fix $N = 2$ in equation (3.4)) between one selected party and all the other $N - 1$ users, and then 
use the established secret keys to encode the final conference key via one-time pad encryption. In this case the 
the asymptotic conference key rate would be $r(2)/(N - 1)$ according to the reasoning given at the beginning of 
section 4, where $r(N)$ is given in (3.4). More generally, it might be advantageous to group the $N$ parties in subsets 
of equal cardinality, let them perform the CKA within the subset, and then use the secret keys established in each 
subset to encode the conference key. Since one selected party must belong to every subset in order to distribute 
the final conference key to the others in a secure way, there are $(N - 1)/d$ subsets of $d + 1$ users each. In this 
case the asymptotic conference key rate would read: $d \cdot r(d + 1)/(N - 1)$. In order to investigate which of 
these configurations yields the highest asymptotic conference key rate, we optimize the rate with respect to the 
possible subdivisions of the $N$ parties in groups of equal cardinality (i.e. we maximize it with respect to all the 
divisors $d$ of $N - 1$):

$$
\frac{d}{dN - 1} \frac{d + 1}{r(N - 1)}
$$

which includes the cases where the parties are iteratively performing bipartite protocols ($d = 1$) and where the $N$
parties are performing the CKA all at once like in figure 2 ($d = N - 1$).

In figure C1(a) we plot the optimized conference key rate for $N = 5$ parties (equation (C.1), solid lines) as a 
function of the loss in each quantum channel, for different values of the parameter $q$ and a fixed number of 
port of the beam splitter: $M = 5$. We also plot the direct transmission bound (4.1) for the same
number of parties. The correspondent optimal number of parties within each subset depends on the loss and on 
the value of $q$, and it is given in figure C1(b).

From figure C1(a) we observe that the resulting key rate, although not being optimized over the parameter $q$, 
is similar to the $N = 5$ key rate in figure 2 for most losses, since we fixed $q$ to values close to the optimal ones.
Furthermore, it performs better than the standard CKA with five parties in the high-loss region. Indeed, as 
already explained in figure 2, the effect of dark counts becomes greater when more parties are performing the 
the same time. Thus, allowing for a lower number of parties within each subset increases the maximum 
tolerated loss.

In figure C1(b) we observe that at low losses it is optimal for the five parties to perform a truly multiparticle 
scheme rather than iteratively performing bipartite protocols. The reason is that in the ideal scenario of 
 extremely low losses ($t \rightarrow 1$) and $q$ close to 1, there is only one party successfully sending one photon to the 
the central node to be detected. In this case the post-selected state shared by the parties is the $W$-class state used for 
establishing the secret key. Of course, there are more chances that this event is going to happen when more 
parties are involved, thus a multiparticle scheme is advantageous with respect to an iteration of bipartite schemes. 
One can see this also analytically, by showing that the asymptotic rate (3.4) of the CKA performed by $N$ parties all 
at once can be approximated as follows (when the above assumptions hold):

$$
r(N) \approx Nq^{N-1}(1-q)t \left[ 1 - \left( \frac{1}{2} - \frac{1}{N} \right) \right]^{N-1}.
$$
while the rate achieved by subdividing the task in $N-1$ bipartite schemes is:

$$r_{\text{bipartite}}(N) \simeq \frac{2q(1-q)t}{N-1}.$$  \hspace{1cm} (C.3)

By numerically comparing (C.2) with (C.3) for sufficiently high values of $q$, one notices that the former results in a higher key rate. When the value of $q$ decreases, the probability that two or more parties send their photon to the central node increases, reducing the key rate. Being such events more likely when more parties are involved, the iterative execution of bipartite schemes is favored. Similarly, increasing the loss transforms the same events—which are more likely with more parties—from neglected events (if they cause double clicks) to harmful events (when some photons get lost in the transmission), thus favoring the iteration of schemes with a low number of parties.

**ORCID iDs**

Federico Grasselli @ https://orcid.org/0000-0003-2966-7813

**References**

[1] Gisin N and Thew R 2007 Nat. Photon. 1 165–71
[2] Kimble H J 2008 Nature 453 1023
[3] Bennett C H and Brassard G 1984 Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing pp 175–9
[4] Ekert A K 1991 Phys. Rev. Lett. 67 661
[5] Scarani V, Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 Rev. Mod. Phys. 81 1301
[6] Lo H-K, Curty M and Tamaki K 2014 Nat. Photon. 8 595–604
[7] Diamanti E, Lo H-K, Qi B and Yuan Z 2016 NPJ Quantum Inf. 2 16025
[8] Pirandola S et al 2019 arXiv:1906.01645
[9] Lo H-K, Curty M and Qi B 2012 Phys. Rev. Lett. 108 130503
[10] Abruzzo S, Kampermann H and Bruß D 2014 Phys. Rev. A 89 012301
[11] Panayi C, Razavi M, Ma X and Lütkenhaus N 2014 New J. Phys. 16 043005
[12] Azuma K, Tamaki K and Munro W J 2015 Nat. Commun. 6 10171
[13] Vazirani U and Vidick T 2014 Phys. Rev. Lett. 113 140501
[14] Friedman R A, Dupuis F, Fawzi O, Renner R and Vidick T 2018 Nat. Commun. 9 459
[15] Yin H-L et al 2016 Phys. Rev. Lett. 117 190501
[16] Boaron A et al 2018 Phys. Rev. Lett. 121 190502
[17] Liao S-K et al 2017 Nature 549 43
[18] Takenaka H et al 2017 Nat. Photon. 11 502
[19] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 Nature 557 400
[20] Tamaki K, Lo H-K, Wang W and Lucamarini M 2018 arXiv:1805.05511
[21] Ma X, Zeng P and Zhou H 2018 Phys. Rev. X 8 031043
