Quantum Conference Key Agreement: A Review

Gláucia Murta, Federico Grasselli, Hermann Kampermann, and Dagmar Bruß *

Conference key agreement (CKA), or multipartite key distribution, is a cryptographic task where more than two parties wish to establish a common secret key. A composition of bipartite quantum key distribution protocols can accomplish this task. However, the existence of multipartite quantum correlations allows for new and potentially more efficient protocols, to be applied in future quantum networks. Here, the existing quantum CKA protocols based on multipartite entanglement are reviewed, both in the device-dependent and the device-independent scenario.

1. Introduction

Quantum mechanics can bring unprecedented advantages to the realization of information processing tasks. A remarkable example is quantum key distribution (QKD),[1,2] arguably the most mature quantum technology. QKD allows two parties, Alice and Bob, to securely communicate by establishing a secret key that is information theoretically secure. Security proofs are given for different levels of assumptions. In the scenario where the devices and/or quantum states are characterized, robust security is proven for realistic parameters[3,4] (see also ref. [5]) with implementations achieving long distances.[6–8] Also for the device-independent scenario, that is, no assumptions on the quantum states and on the working behavior of the devices, a security proof in the fully adversarial scenario is well established[9] (barring composability in case the devices are re-used, see Remark 1). The required experimental parameters are characterized[10] for protocols based on the simplest Bell inequality.[11]

The extensive development of quantum technological applications allows near future applications which are based on genuine multipartite quantum protocols using shared multipartite entangled states in network structures.[12–18] Applications range from distributed quantum computing to genuine multipartite quantum communication protocols which may lead to the quantum internet.[19,20]

Here we focus on conference key agreement (CKA), or multiparty key distribution, which is a generalization of the task of key distribution to the scenario in which N users wish to establish a common secret key. This allows the users to broadcast secure messages in a network. CKA can e.g. be achieved by, first establishing bipartite keys between the users, followed by securely distributing a common key to all other users via the bipartite keys. This solution has been discussed to be inefficient in the classical scenario, and several classical protocols allowing the parties to establish a common key were proposed (see e.g., refs. [21, 22] and [23, 24]). In the quantum scenario, that is, when the parties can use quantum resources, a secure conference key can also be established by using several bipartite QKD links. Bipartite quantum links are already being implemented in small quantum networks over metropolitan distances[25–31] and in larger networks spanning entire countries.[32–34] The long-term vision of a general quantum network, however, goes beyond mere bipartite links and includes network nodes that process quantum information, thus enabling the distribution of multipartite entangled states across the network.[12] In a quantum network, quantum communication with genuine multipartite entangled states may offer advantages over the bipartite case,[35] and allow secure interactions between an arbitrary subset of the participating partners.

The rich structure of multipartite entangled quantum states opens the possibility for a wide variety of new key distribution protocols. While protocols for CKA based merely on bipartite QKD do not bring much novelty in terms of the necessary quantum technologies or the theoretical tools required for the security analysis, this changes when protocols explore multipartite entanglement. Here, quantum correlations can be exploited to devise truly multipartite schemes. This is the focus of this paper, namely we will review the proposals and developments regarding the use of multipartite quantum entanglement for the establishment of a conference key.

2. Preliminaries

2.1. Multipartite Entangled Resources

Multipartite quantum states have a more convoluted structure than the bipartite ones.[36–39] Different classes of states can be defined according to their entanglement properties, and concepts such as k-separability and genuine multipartite entanglement arise (for a precise definition of these concepts, see refs. 36, 37, 39]). For multipartite systems, there exist different entanglement classes that are not equivalent under stochastic local operations and classical communication (SLOCC).[39–41] In

Dr. G. Murta, Dr. F. Grasselli, Dr. H. Kampermann, Prof. D. Bruß
Institut für Theoretische Physik III
Heinrich-Heine-Universität Düsseldorf
Universitätsstraße 1
Düsseldorf D-40225, Germany
E-mail: dagmar.bruss@uni-duesseldorf.de

The ORCID identification number(s) for the author(s) of this article can be found under https://doi.org/10.1002/qute.202000025

DOI: 10.1002/qute.202000025

particular, in the tripartite case,[40] two nonequivalent classes of genuinely multipartite entangled states can be defined: the GHZ-class represented by the Greenberger–Horne–Zeilinger (GHZ) state[42]

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \tag{1}$$

and the W-class represented by the W state[40]

$$|\mathrm{W}\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle) \tag{2}$$

These classes of states also exhibit different physical properties. The GHZ-state is a direct generalization of Bell states to the multipartite case and maximally violates the well-studied family of N-party Bell inequalities called MABK.[43–45] However, the entanglement present in the GHZ-state is not robust to particle losses, while the W-state still exhibits bipartite entanglement when one particle is lost.

The 3-party GHZ and W states in Equations (1) and (2) can be generalized in a straightforward way to N parties. They constitute the resources for quantum CKA protocols discussed in the following sections.

2.2. Security

2.2.1. Security Definition

We consider N users, Alice, Bob$_1$, Bob$_2$, ..., Bob$_{N-1}$. The users wish to establish a common string of bits that is unknown to any other party, in particular to any potential eavesdropper.

The security of a quantum conference key agreement protocol is based on two conditions: correctness and secrecy.

Definition 1 (Correctness). *A CKA protocol is ϵ_{corr}-correct if*

$$p(K_A = K_{B_1} = \cdots = K_{B_{N-1}}) \geq 1 - \epsilon_{\mathrm{corr}} \tag{3}$$

where K_A, K_{B_i} are the final keys held by Alice and Bob$_i$ and $p(K_A = K_{B_1} = \cdots = K_{B_{N-1}})$ is the probability that all final keys are identical.

Definition 2 (Secrecy). *A CKA protocol is ϵ_{sec}-secret if, for Ω being the event that the protocol does not abort,*

$$p(\Omega)\frac{1}{2}\|\rho_{K_A E|\Omega} - \tau_{K_A} \otimes \rho_{E|\Omega}\| \leq \epsilon_{\mathrm{sec}} \tag{4}$$

where $p(\Omega)$ is the probability of the event Ω, $\rho_{K_A E|\Omega}$ is the state shared by Alice and Eve at the end of the protocol given the event Ω, $\tau_{K_A} = \frac{1}{|S|}\sum_{s_i \in S} |s_i\rangle\langle s_i|$ is the maximally mixed state over all possible values that the key K_A can assume, and $S = \{0,1\}^{\times \ell}$ where ℓ is the length of the key K_A.

Correctness implies that, at the end of the protocol, Alice and the Bobs share the same string of bits except for probability at most ϵ_{corr}. The secrecy requirement states that Alice's key is randomly chosen among the set of possible strings and the eavesdropper has no information about the key, except for probability at most ϵ_{sec}. If a CKA protocol is ϵ_{corr}-correct and ϵ_{sec}-secret, then it is said to be ϵ_s-correct-and-secret for all $\epsilon_s \geq \epsilon_{\mathrm{corr}} + \epsilon_{\mathrm{sec}}$.

Additionally, a useful CKA protocol should have a robust honest implementation. This is captured by the concept of completeness.

Definition 3 (Completeness). *A quantum CKA protocol is ϵ_c-complete if there exists an honest implementation of the protocol, such that the probability of not aborting is greater than $1 - \epsilon_c$.*

Finally, the security of a quantum CKA protocol can be summarized as [46]:

Definition 4 (Security of a quantum CKA protocol). *A quantum CKA protocol is (ϵ_s, ϵ_c)-secure if*

(I) (Soundness) For any implementation of the protocol, it is ϵ_s-correct-and-secret.
(II) (Completeness) There exists an honest implementation of the protocol, such that the probability of not aborting is greater than $1 - \epsilon_c$.

Definition 4 implies composable security.[46–48] This means that the conference key generated by a protocol satisfying the conditions stated in Definition 4 is composable secure and therefore can be used as a building block for further protocols (this, however, cannot always be inferred in the device-independent scenario, see Remark 1 in Section 5).

The quantum left-over hashing lemma[49,50] establishes that a secret conference key can be obtained if the key length ℓ is slightly shorter than

$$\ell \lesssim H^{\epsilon}_{\min}(A_1^n|E) \tag{5}$$

where $H^{\epsilon}_{\min}(A_1^n|E)$ is the conditional smooth min-entropy[51] evaluated for the classical-quantum (cq) state $\rho_{A_1^n E}$ composed of Alice's raw key of size n and the quantum side information of a potential eavesdropper.

The conditional smooth min-entropy of a cq-state ρ_{AE} is defined as

$$H^{\epsilon}_{\min}(A|E) = \sup_{\tilde{\rho}_{AE} \in \mathcal{B}^{\epsilon}(\rho_{AE})} H_{\min}(A|E) \tag{6}$$

where $\epsilon \in [0,1)$, and the supremum is taken over positive subnormalized operators that are ϵ-close to ρ_{AE} in the purifying distance,[51] and the conditional min-entropy, $H_{\min}(A|E)$, of a classical variable A conditioned on the quantum side information E is closely related to the optimal probability of the eavesdropper guessing the value of A, $p_{guess}(A|E)$[52]

$$H_{\min}(A|E) = -\log p_{guess}(A|E) \tag{7}$$

For a precise definition and properties of entropic quantities we refer the reader to ref. [51].

The main task in the security proof of a conference key agreement protocol is to estimate $H^{\epsilon}_{\min}(A_1^n|E)$. Note that this is very similar to the bipartite case of quantum key distribution. In fact, the secrecy condition only depends on the correlations between the eavesdropper and Alice's string. However, in the multipartite scenario the parties need to ensure that all of the Bobs correct their raw key so that the correctness requirement is satisfied.

2.2.2. Security Model

In the scenario where N parties wish to securely communicate, the adversary is an external party, Eve, who can eavesdrop on all the exchanged public communication. Moreover, Eve might try to tamper with the quantum channels and explore correlations with the generated conference key.

Similar to the bipartite case, we can also classify the attacks performed by the eavesdropper into three categories:

1. *Individual attacks*: the eavesdropper can only attack individually each round of the protocol. In this case she is assumed to have no quantum memory, and therefore her best strategy is to perform a measurement on her quantum side information at each round.
2. *Collective attacks:* Eve is assumed to perform the same attack for each round of the protocol, that is, her quantum side information is identically and independently distributed (IID) with respect to different rounds. Differently from individual attacks, Eve is now assumed to have a quantum memory. Therefore, she can store her quantum side information at each round and perform a global operation on it at the end of the execution of the protocol.
3. *Coherent attacks:* This is the most general type of attack where there are no assumptions on the capabilities of the eavesdropper, except that she is bounded by the laws of quantum mechanics. In this case, the states shared by the parties at each round may have arbitrary correlations with previous and future rounds.

2.3. Generic Protocols

The goal of quantum conference key agreement is that the N users make use of their shared quantum resources together with local operations and public communication in order to establish a secure conference key.

In the following section, we will present the proposed quantum protocols that perform the task of CKA, making use of multipartite entanglement. The protocols we will discuss consist of the following main steps:

1. *Preparation and distribution:* A source distributes a multipartite entangled state to the N parties. This step is repeated n times.
2. *Measurements:* Upon receiving the systems, the parties perform local measurements and record the classical outcome. The measurements are randomly chosen according to the specifications of the protocol. One of the possible measurement settings is used with higher probability and is called the *key generation* measurement. The other measurements are used for *test rounds,* which only occasionally occur. A short preshared key can be used to determine if a round is a key generation round or a test round. Alternatively, the parties can implement a sifting step[5] to select rounds where the same type of measurements were performed.
3. *Parameter estimation*: The parties announce the inputs and outputs of their test rounds and of some randomly chosen key generation rounds which are used to estimate their correlation and the potential influence of an eavesdropper. At the end of this step, each party is left with a string of $n_{\text{raw}} < n$ bits, which constitute their raw key.
4. *Information reconciliation (error correction):* The parties publicly exchange classical information in order for the Bobs to correct their raw keys to match Alice's string. In the multipartite case, the information reconciliation protocol needs to account for the correction of the strings of all the Bobs.
5. *Privacy amplification*: Alice randomly picks a hash function, chosen among a two-universal family of hash functions (see ref. [49]), and communicates it to the Bobs. Every party applies the hash function to turn her/his partially secure string of n_{raw} bits into a secure key of $\ell < n_{\text{raw}}$ bits.

The key rate of a protocol is given by

$$r = \tau \frac{\ell}{n} \tag{8}$$

where τ is the repetition rate of the setup, that is, the inverse of the time it takes to implement one round of preparation and measurement of the quantum systems. In the following sections, we will typically take $\tau = 1$ as we will not be focused on any specific experimental implementation. The key rate in the limit of infinitely many rounds, $n \to \infty$, is called the asymptotic key rate and denoted r_∞.

3. Protocols for Multi-Qubit States

3.1. GHZ State Protocols

The first proposals of quantum conference key agreement protocols explore the multipartite correlations exhibited by the N-party GHZ state:

$$|\text{GHZ}_N\rangle = \frac{1}{\sqrt{2}}(|00\ldots0\rangle + |11\ldots1\rangle) \tag{9}$$

where $\{|0\rangle, |1\rangle\}$ is the Z-basis, composed by the eigenstates of the Pauli operator σ_z. The GHZ state satisfies all the desired conditions for a conference key agreement protocol: the outcomes of measurements in the Z-basis are perfectly correlated, random and uniformly distributed. Interestingly, for $N \geq 3$, this perfect correlation can only be achieved if all the parties measure in the Z-basis. As shown in ref. [35], even bipartite perfect correlation cannot be obtained if the parties choose a different basis. This represents a drastic difference from the bipartite case ($N = 2$). Indeed, if Alice and Bob share the maximally entangled state $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, for each choice of local basis for Alice, there exists a local basis for Bob such that their outcomes exhibit perfect correlation. This property is exploited in the bipartite six-state[53] and BB84[1] protocols for QKD.

Early proposals of protocols that employ the GHZ state to establish a conference key between three parties were presented in ref. [54]. Security is proved, against individual attacks, for the ideal case where Alice can prepare and distribute perfect GHZ states. Robustness to noise is not considered. In ref. [55], Chen and Lo proved the security of quantum conference key agreement based on the distillation of GHZ states.[56,57] They derive distillation rates for a protocol based on an improved version of the multi-party hashing method.[56] These rates correspond to conference key rates, due to the fact that the multi-party hashing distillation protocol[56] can be implemented by classical post-processing of the raw key. Ref. [55] also considers distillation rates when recurrence protocols are applied before the multi-party hashing. Recurrence protocols are based on CSS codes[58,59] and, if certain conditions are met, they can also be translated to a classical post-processing of the generated raw keys, in a similar fashion to the bipartite case.[60] Ref. [55] modifies the recurrence protocol introduced in ref. [57], using ideas of ref. [60], to design a protocol that can be converted to classical post-processing of the raw key. This type of classical post-processing of the raw key requires two-way communication and was denoted advantage distillation.[61–63]

In the following subsections, we present specific protocols with GHZ states that can be regarded as the generalization of the six-state and the BB84 protocols to the multipartite case.

3.1.1. Multiparty Six-State Protocol

The quantum conference key agreement protocol introduced in ref. [35] can be seen as a generalization of the six-state QKD protocol[53] to the multipartite case. Indeed, in ref. [35], the parties perform measurements in the three bases $\{X, Y, Z\}$. Measurements in the Z-basis are used with higher frequency, and they constitute the key generation rounds. The X-basis and Y-basis are instead used in fewer rounds, specifically in the test rounds, in order to estimate the information available to a potential eavesdropper.

From the parameter estimation rounds, the statistics of the Z-measurements is used to estimate the qubit error rates (QBERs) and thus to determine the information that needs to be communicated by Alice for information reconciliation. The bipartite QBERs, Q_{AB_i}, for $1 \leq i \leq N-1$, are the probabilities that the outcome of a Z-measurement by Bob$_i$ disagrees with Alice's Z-measurement outcome. In the multipartite scenario we can also define the total QBER Q_Z as the probability that at least one Bob obtains an outcome different than Alice. If the N parties share a state ρ, the QBER Q_Z is given by

$$Q_Z = 1 - \mathrm{tr}\left(\rho\big(|0\rangle\langle 0|^{\otimes N} + |1\rangle\langle 1|^{\otimes N}\big)\right) \tag{10}$$

With the statistics of the test rounds, the parties want to estimate the expected value of the operator $X^{\otimes N}$. Since the multipartite GHZ state does not exhibit perfect correlation in more than one basis,[35] the QBER Q_X is defined as the probability that the $X^{\otimes N}$-measurement gives a result that differs from the ideal case:

$$Q_X = \frac{1 - \langle X^{\otimes N}\rangle}{2} \tag{11}$$

Note that if the parties share the GHZ state (9), then the corresponding Q_X is zero.

A crucial step in the security analysis of the protocol presented in ref. [35] is a reduction to depolarized states. An N-qubit depolarized state is a state of the form

$$\begin{aligned}\rho_{\mathrm{dep}} = {} & \lambda_{0,\vec{0}}|\psi_{0,\vec{0}}\rangle\langle\psi_{0,\vec{0}}| + \lambda_{1,\vec{0}}|\psi_{1,\vec{0}}\rangle\langle\psi_{1,\vec{0}}| \\ & + \sum_{\sigma,\vec{u}\neq\vec{0}} \lambda_{\vec{u}}|\psi_{\sigma,\vec{u}}\rangle\langle\psi_{\sigma,\vec{u}}|\end{aligned} \tag{12}$$

where

$$|\psi_{\sigma,\vec{u}}\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle|\vec{u}\rangle + (-1)^{\sigma}|1\rangle|\bar{\vec{u}}\rangle\Big) \tag{13}$$

for $\vec{u} \in \{0,1\}^{\times(N-1)}$, $\bar{\vec{u}} = \vec{u} \oplus \vec{1}$, and $\sigma \in \{0,1\}$. The states $\{|\psi_{\sigma,\vec{u}}\rangle\}_{\sigma,\vec{u}}$ form a basis, denoted as the GHZ basis. The depolarized GHZ state is then diagonal in the GHZ basis and such that $\lambda_{0,\vec{u}} = \lambda_{1,\vec{u}} \equiv \lambda_{\vec{u}}$ for $\vec{u} \neq \vec{0}$.

For a state of the form (12), one finds that

$$Q_Z(\rho_{\mathrm{dep}}) = 1 - (\lambda_{0,\vec{0}} + \lambda_{1,\vec{0}}) \tag{14}$$

and

$$Q_X(\rho_{\mathrm{dep}}) = \frac{1 - (\lambda_{0,\vec{0}} - \lambda_{1,\vec{0}})}{2} \tag{15}$$

Finally, the asymptotic key rate for the depolarized state (12) is given as a function of Q_X, Q_Z and the bipartite QBERs Q_{AB_i}[35]

$$\begin{aligned} r_\infty = & (1 - Q_Z)\big(1 - \log(1 - Q_Z)\big) \\ & + \left(1 - \frac{Q_Z}{2} - Q_X\right)\log\left(1 - \frac{Q_Z}{2} - Q_X\right) \\ & + \left(Q_X - \frac{Q_Z}{2}\right)\log\left(Q_X - \frac{Q_Z}{2}\right) \\ & - \max_{1\leq i\leq N-1} h\big(Q_{AB_i}\big)\end{aligned} \tag{16}$$

For the generality of the security analysis of ref. [35], it remains to argue that the reduction to depolarized states, (12), is not restrictive. Any N-qubit state can be brought to the form (12) by successive application of the following set of local operations:[64,65]

$$\begin{aligned}\mathcal{D} = & \left\{X^{\otimes N}\right\} \cup \left\{Z_{AB_j} | 1 \leq j \leq N-1\right\} \\ & \cup \{R_k | 1 \leq k \leq N-1\}\end{aligned} \tag{17}$$

where the operations Z_{AB_j} and R_k are defined as

$$Z_{AB_j} = Z_A \otimes Z_{B_j} \otimes I_{B_{[N-1]\setminus j}} \tag{18}$$

and

$$R_k = \mathrm{diag}(1, i)_A \otimes \mathrm{diag}(1, -i)_{B_k} \otimes I_{B_{[N-1]\setminus k}} \tag{19}$$

Indeed, the application of the map

$$\rho \mapsto \tilde{\rho} = \circ_{i=1}^{2N-1} \mathcal{D}_i[\rho] \tag{20}$$

where

$$\mathcal{D}_i[\rho] = \frac{1}{2}\rho + \frac{1}{2}D_i\rho D_i^{\dagger}\,;\ D_i \in \mathcal{D} \tag{21}$$

brings any N-qubit state to the form (12).

A crucial observation is that the map (20) can be implemented in the protocol by flipping the outcomes of some of the measurements and adding additional measurements in the Y-basis.[35]

Consider first the set of operations $\{X^{\otimes N}\} \cup \{Z_{AB_j}|1 \leq j \leq N-1\}$. Successive application of these operations brings any N-qubit state to the GHZ-diagonal form

$$\tilde{\rho} = \sum_{\sigma,\vec{u}} \lambda_{\sigma,\vec{u}} |\psi_{\sigma,\vec{u}}\rangle\langle\psi_{\sigma,\vec{u}}| \tag{22}$$

For the key generation rounds, in which Alice and the Bobs measure in the Z-basis, the application of Z_{AB_j} does not have any effect on the final outcomes, and the operation $X^{\otimes N}$ can be equivalently applied by Alice and the Bobs by flipping their Z-measurement outcomes. For the estimation of $X^{\otimes N}$ in the test rounds, the operations $\{X^{\otimes N}\} \cup \{Z_{AB_j}|1 \leq j \leq N-1\}$ have no effect, as can be seen by the fact that they commute with $X^{\otimes N}$.

The application of the operations $\{R_k\}$ is what finally brings the state to the depolarized form (12). They have no effect on the key generation rounds as they do not change the outcome of the Z-measurements. For the test rounds, the action of R_k is more subtle. As shown in ref. [35], the action of R_k followed by a measurement in the X-basis is equivalently implemented by Bob$_k$ performing a Y-basis measurement. Therefore the action of the operators $\{R_k\}$, which are essential to simplify the security analysis of the protocol introduced,[35] can be implemented in the protocol by adding Y-basis measurements to the test rounds.

In ref. [35], the authors show that in a quantum network with quantum routers, for a bottleneck configuration with constrained channel capacity, the multipartite six-state protocol based on the GHZ state leads to higher rates as compared to several implementations of bipartite QKD, when the gate quality is above certain threshold value.

A security analysis of the multiparty six-state protocol against coherent attacks taking into account finite size effects was presented in ref. [66].

3.1.2. Multiparty BB84 Protocol

In ref. [66], also a multipartite version of the BB84 protocol was introduced: Here, the parties only need to perform measurements in two bases, the Z-basis and the X-basis. The security analysis is based on the uncertainty relation for smooth entropies.[67] This technique has previously been used in the bipartite case[3,5] for the security proof of the BB84 protocol in the finite regime for parameters that are compatible with current technology. The uncertainty relation establishes that for a pure state $|\psi_{A\vec{B}E}\rangle$, if Alice can perform measurements in two bases, say the X-basis and the Z-basis, then the following relation is satisfied:

$$H^{\epsilon}_{\min}(Z_1^m|E) \leq q - H^{\epsilon}_{\max}(X_1^m|B_1 \ldots B_{N-1}) \tag{23}$$

where the conditional smooth min-entropy on the l.h.s. is evaluated for the cq-state shared by Alice and Eve when Alice measures her systems in the Z-basis, and the conditional smooth max-entropy on the r.h.s. is evaluated for the cq-state shared by Alice and the Bobs when Alice measures her systems in the X-basis. For a precise definition of $H^{\epsilon}_{\max,}$ we refer the reader to ref. [51]. The term q quantifies the incompatibility of the two measurements used by Alice, and for the case where Alice can measure X or Z the quality factor q for the m rounds will be equal to m.

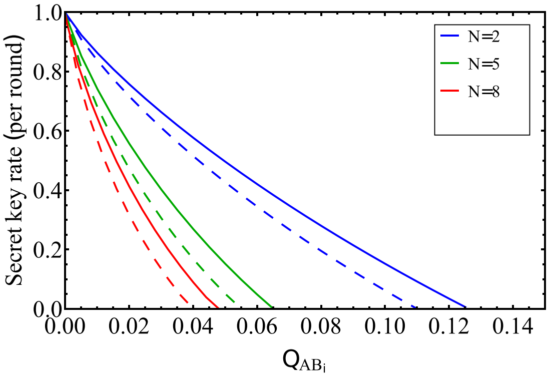

Figure 1. Asymptotic secret key rates of the multipartite six-state (solid)[35] and BB84 (dashed)[66] protocols as a function of the bipartite QBER between Alice and any Bob, for a local depolarizing noise model. The rates are plotted for different numbers of parties ($N = 2, 5, 8$, right to left). The plot shows that the multipartite six-state protocol asymptotically outperforms the multipartite BB84 protocol.

The quantity $H^{\epsilon}_{\max}(X_1^m|B_1 \ldots B_{N-1})$ can be estimated by using the X-measurements performed by the Bobs (11). Indeed, the data processing inequality guarantees that

$$H^{\epsilon}_{\max}(X_1^m|B_1 \ldots B_{N-1}) \leq H^{\epsilon}_{\max}(X_1^m|\vec{X}_1^m) \tag{24}$$

where $\vec{X}_1^m$ contains the X-outcomes of every Bob, had the Bobs measured in the X-basis in the m rounds. Clearly the entropy on the r.h.s. of Equation (24), that is the entropy of Alice's X-outcome string given the X-outcome strings of the Bobs, can be estimated via the X-basis error defined in Equation (11).

Finally ref. [66] establishes the asymptotic secret key rate of the multiparty BB84 protocol

$$r_{\infty} = 1 - h(Q_X) - \max_{1 \leq i \leq N-1} h(Q_{AB_i}) \tag{25}$$

3.1.3. Comparison of Multiparty Six-State and BB84 Protocols

For any specific implementation, the asymptotic key rates obtained by the multiparty six-state protocol[35] are higher than those obtained by the multiparty BB84.[66] This is because more structure can be ensured about the underlying state in the protocol presented in ref. [35]. For instance, consider the implementation where Alice prepares a GHZ state and distributes it to each of the Bobs using a qubit depolarizing channel. The state shared by the parties is thus

$$\rho_{A\vec{B}} = \mathcal{D}_2^{\otimes(N-1)} |\text{GHZ}_N\rangle\langle\text{GHZ}_N| \tag{26}$$

where

$$\mathcal{D}_2(\rho) = (1-\nu)\rho + \nu\frac{\mathbb{1}}{2} \tag{27}$$

Figure 1 shows the comparison of the asymptotic key rates achieved by the two multiparty protocols ($N = 2, 5, 8$) in the specific implementation given by the noise model in Equation (26).

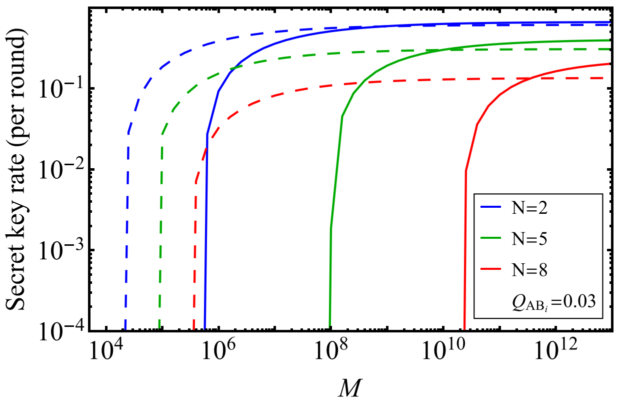

Figure 2. Secret key rates of the multipartite six-state (solid)[35] and BB84 (dashed)[66] protocols as a function of the total number of rounds M, for different number of parties ($N = 2, 5$, and 8, left to right) and fixed bipartite QBER ($Q_{AB_i} = 0.03$). The noise model employed is the local depolarizing channel given in Equations (26) and (27). A non-null conference key can be obtained for fewer rounds with the multipartite BB84 protocol, compared to the multipartite six-state protocol, and the advantage of the former protocol increases with the number of parties.

The key rates are plotted as a function of the bipartite QBER between Alice and any Bob, which turns out to be a simple function of the noise parameter characterizing the depolarizing channel: $Q_{AB_i} = \nu/2$. The figure confirms that, asymptotically, the multipartite six-state protocol[35] overcomes the multipartite BB84[66] in terms of performance.

Ref. [66] also performs a complete security analysis in the finite-key regime for the multiparty six-state and multiparty BB84 protocol. Regarding the rates in the finite-key regime, it was shown that, even though the six-state protocol can tolerate higher noise, for the low-noise regime, a non-zero conference key rate can be proven for the multiparty BB84 protocol using a significantly smaller number of rounds. This is confirmed by **Figure 2**, where the secret key rates of both protocols are plotted as a function of the total number of protocol rounds, having fixed the bipartite QBER. The noise model employed is the same used for Figure 1, that is the local depolarizing channel given in Equation (27). It is important to remark that the lower threshold on the minimum number of signals for a non-zero key by the multiparty BB84 protocol, may be simply due to the techniques used to compute the key rates. The finite-key rates of the multipartite six-state are derived using the post-selection technique[68] in combination with the finite version of the asymptotic equipartition property[69] (see also ref. [49]). These techniques might lead to higher overhead terms in the finite-key regime and therefore to a less tight estimate than what can be obtained using the uncertainty relation for smooth entropies.[67] However, due to the fact that in the multiparty six-state protocol the parties are required to perform three distinct measurements, the uncertainty relation is not applicable.

3.1.4. Prepare-and-Measure Implementation

Even though entanglement plays an essential role for the security of bipartite QKD, it is known that some QKD protocols have a corresponding prepare-and-measure implementation that does not require any entanglement. The BB84 protocol, for example, can be implemented with Alice transmitting single qubit states to Bob.

Similarly, in the multipartite case, we can also talk about a corresponding prepare-and-measure implementation. However, now this reduction will require the preparation of some $(N-1)$-entangled states.[35]

Indeed for the key generation rounds, in which the parties are performing measurements in the Z-basis, Alice could instead randomly choose her bit and prepare $(N-1)$ copies of the corresponding single qubit state to send to the Bobs, $|0\rangle^{\otimes(N-1)}$ or $|1\rangle^{\otimes(N-1)}$. Although entanglement is not required to reproduce the statistics of the key generation rounds, the corresponding state shared by the Bobs when Alice performs a measurement in the X-basis or Y-basis is entangled. Therefore, for the test rounds, Alice is required to prepare an $(N-1)$-entangled state.

For example, when Alice performs an X-measurement, given that she obtains the outcome a, the corresponding state that she has to distribute to the Bobs is the $(N-1)$-entangled state

$$|\psi_a\rangle_{B_1\ldots B_{N-1}} = \frac{1}{\sqrt{2}}\big(|00\ldots 0\rangle + (-1)^a|11\ldots 1\rangle\big) \tag{28}$$

The prepare-and-measure equivalence significantly reduces the resources required for the implementation of the protocols,[35,66] as Alice needs to control $(N-1)$-partite entanglement instead of N-partite entanglement. This can have significant practical implications especially in the noisy intermediate scale (NISQ) era.[70] Moreover, it is important to remark that, for most of the rounds, the key generation rounds, Alice can in fact prepare product states, and entanglement is only required in a small fraction of the rounds for the purpose of parameter estimation.

A prepare-and-measure protocol in which Alice only needs to send separable states was proved secure for the case $N = 3$ in ref. [71]. However, when extending the protocol to an arbitrary number of parties N the states distributed by Alice would become increasingly distinguishable as N increases, which would allow an eavesdropper to retrieve more information about the key, while causing less disturbance. Thus, the secret key rate would decrease with increasing N, even for a perfect implementation.

3.2. *W* State Protocol

Quantum conference key agreement does not necessarily need to rely on the correlations provided by multipartite GHZ states. Indeed, the protocol devised in ref. [72] exploits the multipartite entanglement of a W-class state in order to establish a conference key. The W state of N parties is defined as

$$|\mathrm{W}_N\rangle = \frac{1}{\sqrt{N}}(|0\ldots 01\rangle + |0\ldots 10\rangle + \cdots + |1\ldots 00\rangle) \tag{29}$$

whereas a W-class state has a similar form to (29) but presents arbitrary phases on each term.

In the conference key agreement protocol of ref. [72], the state is post-selected thanks to single-photon interference occurring in a central untrusted node, extending the founding idea of twin-field QKD[73,74] to the multipartite scenario.

In particular, each round of the protocol starts with party$_i$ ($i = 1, 2, \dots, N$) preparing the following entangled state between an optical pulse a_i and a qubit A_i:

$$|\phi\rangle_{A_i a_i} = \sqrt{q}|0\rangle_{A_i}|0\rangle_{a_i} + \sqrt{1-q}|1\rangle_{A_i}|1\rangle_{a_i} \tag{30}$$

where $|0\rangle_{a_i}$ 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 the qubit. The state is strongly unbalanced towards the vacuum: $q \approx 1$. Every party sends his/her optical pulse to a central untrusted node through a lossy optical channel. Here, the pulses are combined in a balanced multiport beam splitter[75] featuring a threshold detector at every output port. The central node announces whether each detector clicked or not and the parties only keep the rounds where exactly one detector clicked. These events are likely to be caused by the arrival and detection of just one photon, due to the unbalance toward the vacuum of the prepared state (30). Because of the balanced superposition generated by the multiport beam splitter, the detected photon could be sent by any party with equal probability. Thus, the main contribution to the N-qubit state shared by the parties conditioned on the single 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. The qubits' relative coefficients have all equal weights but contain complex phases introduced by the multiport beam splitter.

It has been proven that the only multiqubit state yielding perfectly correlated and random outcomes upon performing local measurements is the GHZ state.[35] Nevertheless, the post-selected W-class state can still be used to distil a conference key. More specifically, the parties obtain the key bits by measuring their qubit in a specific direction in the X-Y plane of the Bloch sphere. The direction is the one that minimizes the bipartite QBER and depends on which detector clicked. For this reason, the protocol cannot be recast as a prepare-and-measure scheme, unlike its bipartite counterpart.[74] Finally, the parties estimate the eavesdropper's knowledge by computing the expectation value of the $Z^{\otimes N}$ operator and by checking when it differs from the ideal case. Note that if the parties are actually sharing a W-class state, then $\langle Z^{\otimes N}\rangle = -1$.

In ref. [72], the security of the protocol is proved in the finite-key regime and under coherent attacks performed by the eavesdropper.

The W-class N-qubit state on which the protocol is based is post-selected thanks to single-photon interference at the central node. Hence, the resulting key rate scales linearly with the transmittance t of one of the quantum channels linking each party to the central node (if the channels are all symmetric). This contrasts with the honest implementations of the protocols[35,66] presented in Section 3.1, which are based on the distribution of N-qubit GHZ states. If these states are encoded, for example, in the orthogonal polarizations of a photon, their key rate cannot scale better than t^N, where t is the transmittance of the link between one party and the central distributor of the N-partite entangled state. This makes the protocol based on the W state much more suited to high-loss scenarios than the protocols of Section 3.1. This is clear from **Figure 3**, where we plot the asymptotic conference key rates of protocols[72] (solid lines) and[35,66] (dashed lines) as a function of the loss in the quantum channel linking one party to the central node ($-10\log_{10} t$). We assume ideal implementations where photon loss is the only source of error. We observe the existence of a loss threshold above which the protocol based on the W state[72] outperforms the protocols based on the distribution of GHZ states.[35,66] Moreover, the required loss for which the protocol[72] outperforms the protocols[35,66] decreases as the number of parties involved increases.

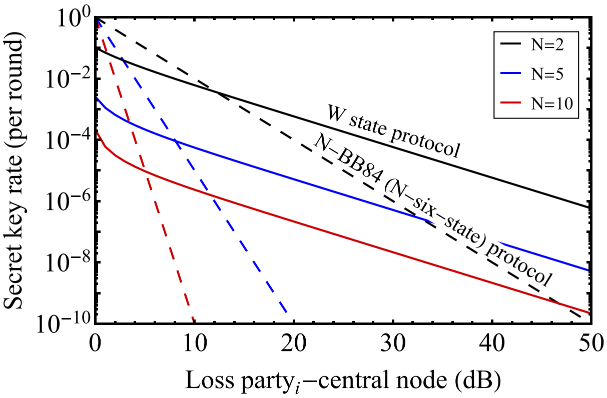

Figure 3. Comparison of the asymptotic conference key rate achieved by the W state protocol[72] (solid) and by the N-BB84 protocol[66] (dashed, the N-six-state protocol rate is identical in this ideal scenario) as a function of the loss in the channel linking each party to the central entanglement distributor, for different number of parties ($N = 2$, 5, and 10). We assume ideal implementations where the only source of error is photon loss and where the GHZ state of the N-BB84 (N-six-state) protocol is encoded in orthogonal polarizations of a photon.

4. Continuous Variable Conference Key Agreement

Quantum conference keys may also be established by means of continuous variable (CV) quantum systems. Following the first of such protocols,[76] which enables quantum conferencing among three parties without trusting the measurement devices, more general and refined protocols[77,78] have been devised. The latter allows an arbitrary number of users to establish conference keys when linked to a central untrusted relay in a star network. These schemes would allow high-rate intra-city secure conferencing among several users.

Both protocols[77,78] rely on the correlations generated by an N-mode CV GHZ state[79]

$$|\text{CVGHZ}\rangle_N = \frac{1}{\sqrt{\pi}}\int_{-\infty}^{\infty} dx|x\rangle^{\otimes N} \tag{31}$$

where $\{|x\rangle\}_x$ are the eigenstates of the $\hat{X}$ quadrature. However, while in ref. [78] the central relay is required to generate such multipartite entangled state, in ref. [77], the state is post-selected thanks to a multipartite CV Bell detection at the central relay. In particular, in ref. [77], every user prepares a Gaussian-modulated coherent state $|\alpha_k\rangle$ ($k = 1, \dots N$) and sends it to the central relay. Here, a suitable cascade of beam splitters followed by homodyne detections of either quadrature $\hat{X}$ or quadrature $\hat{P}$ implement the multipartite Bell detection, whose outcome is made public. The Bell detection projects the incoming coherent states onto the CV GHZ state (31) up to displacements of the N modes. By employing the public data of the Bell detection, the parties post-process the variables $\{\alpha_k\}_{k=1}^N$ describing the prepared coherent states and neutralize the effect of the displacements. They are thus left with variables whose correlations reproduce those of the original CV GHZ state (31) and hence can be used to distil a conference key. This procedure closely resembles the seminal work on measurement-device-independent (MDI) QKD with discrete variables[80][81] and its CV counterpart,[82] now applied to a multipartite scenario. Indeed, the fact that the measurements are only performed by the untrusted relay, makes the protocol in ref. [77] an MDI multipartite QKD protocol. Nevertheless, its performance does not decrease exponentially with the number of users since the CV Bell detection is a deterministic process, unlike its discrete-variable counterpart.[83]

Note that, unlike the discrete-variable scenario, here the correlated variables $\{\alpha_k\}_{k=1}^N$ used to distil a binary key are complex numbers. Nevertheless, one can still express the resulting asymptotic key rate against collective attacks in terms of their mutual information $I(\alpha_k, \alpha_{k'})$[84] with the well-known Devetak–Winter formula.[85]

Compared to ref. [77], the protocol in ref. [78] is not MDI since the multipartite GHZ state generated in the untrusted relay is then distributed to the parties who perform trusted measurements. Moreover, from a practical point of view, this scheme is harder to implement, as it involves the preparation of several optical modes in squeezed states and their subsequent entanglement in a specific target state. Nevertheless, in principle, the scheme in ref. [78] could achieve slightly higher performances than the more practical protocol in ref. [77].

In terms of security, both protocols[77,78] have been proved to be secure against collective Gaussian attacks. Furthermore, the protocol in ref. [77] has been analyzed in the framework of finite-key composable security and proven to be secure against coherent attacks through a Gaussian de Finetti reduction.[86]

5. Device-Independent Conference Key Agreement

In the device-independent scenario, Alice and the Bobs do not want to assume any knowledge about the distributed system and internal working of their devices. Security can even be analyzed under the premise that the shared states as well as the measurement devices were manufactured by the adversary. We note that some assumptions are still present in the device-independent scenario, such as isolated labs and trusted random number generators (see ref. [10] for a discussion). The parties' goal is to ensure security using only the observed statistics of inputs and outputs. In a device-independent protocol security is certified by the violation of a Bell inequality.

Note that in a device-independent conference key agreement (DICKA) protocol, an analysis against coherent attacks also needs to account for the fact that the eavesdropper might program the devices to behave in different ways at each round of the protocol. In particular, the measurement devices could have memory and behave in correlation with the outcomes of previous rounds. This makes the security analysis in the fully device-independent adversarial scenario significantly more intricate.

A recently developed technique,[9,87] the entropy accumulation theorem (EAT), provides the tools to perform the security analysis of device-independent protocols in the fully adversarial scenario maintaining some noise robustness. The EAT[9,87] extends the de Finnetti theorems[68,88] to the device-independent setting, allowing to reduce the analysis to collective attacks.

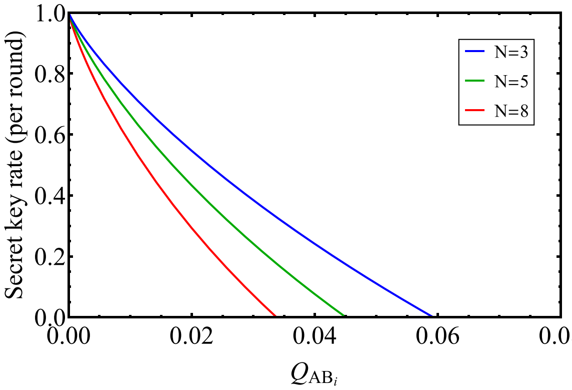

Figure 4. Asymptotic secret key rate for the DICKA protocol of ref. [91] as a function of the QBER and for fixed number of parties ($N = 3, 5, 8$). We assumed an implementation where the N-party GHZ state is submitted to the depolarizing channel $\mathcal{D}_2^{\otimes N}(|\mathrm{GHZ}_N\rangle\langle\mathrm{GHZ}_N|)$.

Remark 1 (Composability in the device-independent scenario). The security definition, Definition 4, implies universal composability of conference key agreement in the trusted device scenario. However, for the device-independent scenario, attacks proposed in ref. [89] show that composability cannot be guaranteed if the same devices are re-used in a subsequent protocol. Indeed, in ref. [89], the authors describe attacks in which information about a previously generated key may be leaked through the public communication of a subsequent run of the protocol, if the devices are re-used. The attacks described in ref. [89] can be avoided if the parties have sufficient control of the internal memory of their devices and are able to re-set it after one execution of the protocol.

Based on the EAT, a DICKA protocol was proposed in refs. [90, 91]. The protocol of ref. [90] initially considers the multipartite Mermin-Ardehali-Belinskii-Klyshko (MABK) inequalities.[43–45] However, as shown in ref. [92], the MABK inequalities are not suitable for establishing a conference key, as an overhead amount of information is required for information reconciliation. In ref. [91], a new multiparty inequality is introduced and positive conference key can be established in the device-independent scenario. **Figure 4** shows the asymptotic key rates for the device-independent protocol of ref. [91] for $N = 3, 5, 8$, for an implementation in which all the qubits are submitted to a depolarizing channel.

The key rates derived in ref. [91] are based on an analytical lower bound to von Neumann entropy of Alice's outcome conditioned on the information available to the eavesdropper, $H(A|E)$, as a function of the violation of the Bell inequality under consideration. The bound employs a relation between the considered multipartite inequality and the bipartite Clauser–Horne–Shimony–Holt (CHSH) inequality.[11]

In general, it is not possible to compute directly $H(A|E)$ as a function of the violation for an arbitrary Bell inequality. This is due to the lack of knowledge about the underlying system. A lower bound can be obtained using the relation $H(A|E) \geq H_{\min}(A|E)$, where $H_{\min}(A|E)$ is the conditional min-entropy defined in (7). Due to the relation with the guessing probability, (7), the conditional min-entropy, $H_{\min}(A|E)$, can be estimated in the device-independent scenario[93] using the hierarchy of semi-definite approximations to the quantum set.[94,95] This method is, however, computationally costly and may lead to non-tight bounds.

Bell inequalities tailored to DICKA protocols were further investigated in [96], where the authors introduced a family of multipartite Bell inequalities (containing the inequality of ref. [91] as a special case) that are maximally violated by the GHZ state, with the Z-basis being one of the optimal measurements for Alice. These are essential features to build a device-independent conference key agreement protocol.

It is interesting to remark that the MABK inequalities were previously explored in other multiparty communication protocols. Refs. [97, 98] consider a secret sharing scenario in which Alice distributes the key in such a way that the $N-1$ Bobs need to collaborate to retrieve its value. The authors establish that, if the eavesdropper is restricted to individual attacks, then the violation of a MABK inequality can guarantee security, even if some of the Bobs collaborate with Eve. Even though this scenario was initially denoted N-party QKD,[97,98] it should be distiguished from the scenario we consider in this review: in which the goal is that all the Bobs can retrieve the key independently.

6. Multipartite Private States

Most of the quantum conference key agreement protocols presented in the previous sections exploit the correlations of the multipartite GHZ state (9). Therefore, GHZ distillation protocols are in close connection with distillation of secret conference keys. Indeed, if the parties share several copies of a resource state that can be turned into a smaller number of GHZ states, then they could perform a distillation protocol followed by measurements to generate a secret key. The connection of entanglement distillation and conference key agreement protocols is discussed in ref. [55].

However, it is not only through distillation of GHZ states that one can obtain a secret key. Indeed, as shown in ref. [99], an ϵ-secure conference key can also be obtained from bound entangled states. This result generalizes an analogous one derived in the bipartite case.[100]

The concept of private states[101] was generalized to the multipartite case in refs. [99, 102]. Similar to the bipartite case, a multipartite private state can be seen as a twisted GHZ state tensored with an extra density matrix (the shield)

$$\Gamma^{(d)}_{A\vec{B}A'} = U_t(|\mathrm{GHZ}^d_N\rangle\langle\mathrm{GHZ}^d_N| \otimes \rho_{A'})\,U_t^\dagger \tag{32}$$

where $|\mathrm{GHZ}^d_N\rangle = \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|ii\dots i\rangle$ is the N-party GHZ state of dimension d and the multipartite twisting is a unitary operation of the form

$$U_t = \sum_{i_1,\dots,i_N=0}^{d-1} |i_1\dots i_N\rangle\langle i_1\dots i_N| \otimes U_{i_1,\dots,i_N} \tag{33}$$

for arbitrary unitaries $U_{i_1,\dots,i_N}$ acting on A'.

Ref. [99] establishes that if from a resource state Alice and the Bobs can distill an ϵ-secret conference key, then there exists an LOCC protocol that can distill a state close to a private state (32) and vice-versa. They also exhibit examples of multipartite bound entangled states, that are states from which a GHZ state cannot be distilled, which are ϵ-close to private states. This establishes that distillation of GHZ states is not necessary for quantum conference key agreement and more general classes of protocols are possible. Limits on the performance of private states distribution in a network, with and without quantum repeaters, and its consequence for CKA protocols, has recently been investigated in refs. [103–105].

In the framework of quantum channels and private state distillation using multiplex channels, ref. [103] establishes that genuine multipartite entanglement is necessary for single shot key distillation. This implies that, if a key can be distilled from n copies of a multipartite state ρ, then $\rho^{\otimes n}$ needs to be genuine multipartite entangled. However, this does not require that genuine multipartite entanglement is present at the single round level ρ. Indeed, a study of the entanglement properties required for a resource state to enable a conference key was recently performed in ref. [106]. Results of ref. [106] show that a conference key can be established even if the parties share a biseparable state in every round.

7. Outlook

We reviewed the state-of-the-art quantum CKA schemes based on multipartite entanglement. We discussed proposed protocols and their security proofs under different levels of assumptions for the characterisation of the devices, and for several types of implementations.

From an experimental point of view, the implementation of quantum CKA is increasingly accessible, due to key developments of its fundamental ingredients. Multipartite entanglement has been generated in a variety of physical systems, such as e.g. ion traps,[107–109] photonic systems,[110–114] superconducting circuits[115–117] and nuclear spin qubits in diamond.[118] Also, entanglement among several particles is naturally generated in atomic ensembles,[119,120] and methods to quantify and manipulate this entanglement are being developed.[121–125] Even a thermalized interacting photon gas[126] has shown potential to be a source of genuine multipartite entanglement. Recently, the first quantum CKA protocol has been implemented[127] among four parties. The experiment is based on the multiparty BB84 protocol[66] discussed in Section 3.1. It relies on the generation of polarization-encoded four-party GHZ states at telecom wavelength by a central quantum server. The states are then distributed to the four parties over up to 50 km of optical fibers, generating a secure conference key according to Definition 4.

While experimental progress is still necessary to scale implementations of quantum CKA to many users, improvements from the theory side are crucial to reduce the experimental demands. To this aim, the development of new protocols and new techniques to prove security will contribute to make quantum CKA a feasible technology.

Novel protocols exploring different resource states and network architectures can lead to improved performance and noise robustness. In the bi-partite case, QKD protocols for d-dimensional systems achieve higher rates and better noise tolerance[128] than the qubit-based protocols. In order to explore this possibility in the multipartite case, quantum CKA protocols for d-dimensional systems need to be developed. Such a generalization can also find applications in the layered protocol presented in ref. [129]. In ref. [129], asymmetric high-dimensional multipartite entangled states are used to design a layered protocol that establishes a secret key simultaneously between different subsets of users in a network.

Similarly, new tools to improve security proofs can lead to better rates and noise tolerance, especially for DICKA protocols. A family of Bell inequalities suitable for conference key agreement protocols has been introduced in ref. [96]. However, only non-tight numerical lower bounds to the key rates are currently available for DICKA protocols based on these inequalities. The introduction of tighter analytical bounds addressing their security proofs could lead to higher key rates in DICKA protocols.

Acknowledgements

The authors thank Giacomo Carrara, Timo Holz, Carlo Ottaviani, Stefano Pirandola, Siddhartha Das, Stefan Bäuml, Marek Winczewski, and Karol Horodecki for helpful discussions. This work was funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy–Cluster of Excellence Matter and Light for Quantum Computing (ML4Q) EXC 2004/1 - 390534769, by the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675662, and by the Federal Ministry of Education and Research BMBF (Project Q.Link.X and HQS).

Open access funding enabled and organized by Projekt DEAL.

Conflict of Interest

The authors declare no conflict of interest.

Keywords

conference key agreement, device-independent protocols, multipartite entanglement, multipartite QKD, quantum cryptography

Received: February 26, 2020
Revised: July 3, 2020
Published online: September 18, 2020

[1] C. H. Bennett, G. Brassard, *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing*, IEEE, Piscataway, NJ **1984**, pp. 175–179.
[2] A. K. Ekert, *Phys. Rev. Lett.* **1991**, *67*, 661.
[3] M. Tomamichel, C. C. W. Lim, N. Gisin, R. Renner, *Nat. Commun.* **2012**, *3*, 634.
[4] M. Hayashi, T. Tsurumaru, *New J. Phys.* **2012**, *14*, 093014.
[5] M. Tomamichel, A. Leverrier, *Quantum* **2017**, *1*, 14.
[6] P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller, J. E. Nordholt, *New J. Phys.* **2006**, *8*, 193.
[7] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, H. Zbinden, *Nat. Photonics* **2015**, *9*, 163.
[8] B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, A. J. Shields, *Optica* **2017**, *4*, 163.
[9] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, T. Vidick, *Nat. Commun.* **2018**, *9*, 459.
[10] G. Murta, S. B. van Dam, J. Ribeiro, R. Hanson, S. Wehner, *Quantum Sci. Technol.* **2019**, *4*, 035011.
[11] J. F. Clauser, M. A. Horne, A. Shimony, R. A. Holt, *Phys. Rev. Lett.* **1969**, *23*, 880.
[12] M. Epping, H. Kampermann, D. Bruß, *New J. Phys.* **2016**, *18*, 053036.
[13] M. Epping, H. Kampermann, D. Bruß, *New J. Phys.* **2016**, *18*, 103052.
[14] F. Hahn, A. Pappa, J. Eisert, *npj Quantum Inf.* **2019**, *5*, 76.
[15] A. Pirker, J. Wallnöfer, W. Dür, *New J. Phys.* **2018**, *20*, 053054.
[16] V. Krutyanskiy, M. Meraner, J. Schupp, V. Krcmarsky, H. Hainzer, B. P. Lanyon, *npj Quantum Inf.* **2019**, *5*, 72.
[17] A. Tchebotareva, S. L. N. Hermans, P. C. Humphreys, D. Voigt, P. J. Harmsma, L. K. Cheng, A. L. Verlaan, N. Dijkhuizen, W. de Jong, A. Dréau, R. Hanson, *Phys. Rev. Lett.* **2019**, *123*, 063601.
[18] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, et al., *Phys. Rev. Lett.* **2018**, *120*, 030501.
[19] H. J. Kimble, *Nature* **2008**, *453*, 1023.
[20] S. Wehner, D. Elkouss, R. Hanson, *Science* **2018**, *362*.
[21] W.-G. Tzeng, in *Public Key Cryptography–PKC 2000*, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg **2000**, pp. 1–13.
[22] Y.-M. Tseng, *Informatica* **2005**, *16*, 275.
[23] S. Berkovits, *Advances in Cryptology — EUROCRYPT '91* (Ed: D. W. Davies), Springer, Berlin, Heidelberg **1991**, pp. 535–541.
[24] G.-H. Chiou, W.-T. Chen, *IEEE Trans Software Eng.* **1989**, *15*, 929.
[25] C. Elliott, *New J. Phys.* **2002**, *4*, 46.
[26] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, H. Yeh, *Quantum Information and Computation III* (Eds: E. J. Donkor, A. R. Pirich, H. E. Brandt), Proc. SPIE Vol. *5815*, SPIE, Bellingham, WA **2005**.
[27] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, et al., *New J. Phys.* **2009**, *11*, 075001.
[28] F. Xu, W. Chen, S. Wang, Z. Yin, Y. Zhang, Y. Liu, Z. Zhou, Y. Zhao, H. Li, D. Liu, Z. Han, G. Guo, *Chin. Sci. Bull.* **2009**, *54*, 2991.
[29] D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J.-B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voirol, N. Walenta, H. Zbinden, *New J. Phys.* **2011**, *13*, 123001.
[30] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, et al., *Opt. Express* **2011**, *19*, 10387.
[31] J. F. Dynes, A. Wonfor, W. W.-S. Tam, A. W. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. L. Yuan, A. R. Dixon, J. Cho, Y. Tanizawa, J.-P. Elbers, H. Greißer, I. H. White, R. V. Penty, A. J. Shields, *npj Quantum Inf.* **2019**, *5*, 101.
[32] R. Courtland, *IEEE Spectrum* **2016**, *53*, 11.
[33] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, et al., *Nature* **2017**, *549*, 43.
[34] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, et al., *Phys. Rev. Lett.* **2018**, *120*, 030501.
[35] M. Epping, H. Kampermann, C. Macchiavello, D. Bruß, *New J. Phys.* **2017**, *19*, 093012.

[36] R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki, *Rev. Mod. Phys.* **2009**, *81*, 865.
[37] O. Gühne, G. Tóth, *Phys. Rep.* **2009**, *474*, 1.
[38] C. Eltschka, J. Siewert, *J. Phys. A: Math. Theor.* **2014**, *47*, 424005.
[39] I. Bengtsson, K. Zyczkowski, arXiv:quant-ph/1612.07747, **2016**.
[40] W. Dür, G. Vidal, J. I. Cirac, *Phys. Rev. A* **2000**, *62*, 062314.
[41] J. I. de Vicente, C. Spee, B. Kraus, *Phys. Rev. Lett.* **2013**, *111*, 110502.
[42] D. M. Greenberger, M. A. Horne, A. Zeilinger, arXiv:quant-ph/0712.0921, **2007**.
[43] N. D. Mermin, *Phys. Rev. Lett.* **1990**, *65*, 1838.
[44] M. Ardehali, *Phys. Rev. A* **1992**, *46*, 5375.
[45] A. V. Belinskiĭ, D. N. Klyshko, *Phys.-Usp.* **1993**, *36*, 653.
[46] C. Portmann, R. Renner, arXiv:quant-ph/1409.3525, **2014**.
[47] R. Canetti, in *Proc. 42nd IEEE Symp. on Foundations of Computer Science*, IEEE, Piscataway, NJ **2001**, p. 136.
[48] M. Ben-Or, D. Mayers, arXiv:quant-ph/0409062, **2004**.
[49] R. Renner, *Int. J. Quantum Inf.* **2008**, *06*, 1.
[50] M. Tomamichel, C. Schaffner, A. Smith, R. Renner, *IEEE Trans. Inf. Theory* **2011**, *57*, 5524.
[51] M. Tomamichel, *Quantum Information Processing with Finite Resources*, SpringerBriefs in Mathematical Physics, Springer, Berlin **2016**.
[52] R. Konig, R. Renner, C. Schaffner, *IEEE Trans. Inf. Theory* **2009**, *55*, 4337.
[53] D. Bruß, *Phys. Rev. Lett.* **1998**, *81*, 3018.
[54] A. Cabello, arXiv:quant-ph/0009025, **2000**.
[55] K. Chen, H. Lo, *Quantum Inf. Comput.* **2007**, *7*, 689.
[56] E. N. Maneva, J. A. Smolin, *Quantum Computation and Information*, Contemporary Mathematics, Vol. *305*, American Mathematical Society, Providence, RI **2002**, pp. 203–212.
[57] M. Murao, M. B. Plenio, S. Popescu, V. Vedral, P. L. Knight, *Phys. Rev. A* **1998**, *57*, R4075.
[58] A. R. Calderbank, P. W. Shor, *Phys. Rev. A* **1996**, *54*, 1098.
[59] A. Steane, *Proc. R. Soc. London, Ser. A* **1996**, *452*, 2551.
[60] D. Gottesman, H.-K. Lo, *IEEE Trans. Inf. Theory* **2003**, *49*, 457.
[61] U. M. Maurer, *IEEE Trans. Inf. Theory* **1993**, *39*, 733.
[62] J. Bae, A. Acín, *Phys. Rev. A* **2007**, *75*, 012334.
[63] B. Kraus, C. Branciard, R. Renner, *Phys. Rev. A* **2007**, *75*, 012316.
[64] W. Dür, J. I. Cirac, R. Tarrach, *Phys. Rev. Lett.* **1999**, *83*, 3562.
[65] W. Dür, J. I. Cirac, *Phys. Rev. A* **2000**, *61*, 042314.
[66] F. Grasselli, H. Kampermann, D. Bruß, *New J. Phys.* **2018**, *20*, 113014.
[67] M. Tomamichel, R. Renner, *Phys. Rev. Lett.* **2011**, *106*, 110506.
[68] M. Christandl, R. König, R. Renner, *Phys. Rev. Lett.* **2009**, *102*, 020504.
[69] M. Tomamichel, R. Colbeck, R. Renner, *IEEE Trans. Inf. Theory* **2009**, *55*, 5840.
[70] J. Preskill, *Quantum* **2018**, *2*, 79.
[71] R. Matsumoto, *Phys. Rev. A* **2007**, *76*, 062316.
[72] F. Grasselli, H. Kampermann, D. Bruß, *New J. Phys.* **2019**, *21*, 123002.
[73] M. Lucamarini, Z. L. Yuan, J. F. Dynes, A. J. Shields, *Nature* **2018**, *557*, 400.
[74] M. Curty, K. Azuma, H.-K. Lo, *npj Quantum Inf.* **2019**, *5*, 64.
[75] M. Zukowski, A. Zeilinger, M. A. Horne, *Phys. Rev. A* **1997**, *55*, 2564.
[76] Y. Wu, J. Zhou, X. Gong, Y. Guo, Z.-M. Zhang, G. He, *Phys. Rev. A* **2016**, *93*, 022325.
[77] R. L. C. Ottaviani, C. Lupo, S. Pirandola, *Commun. Phys.* **2019**, *2*, 118.
[78] Z. Zhang, R. Shi, Y. Guo, *Appl. Sci.* **2018**, *8*.
[79] P. van Loock, A. Furusawa, *Phys. Rev. A* **2003**, *67*, 052315.
[80] H.-K. Lo, M. Curty, B. Qi, *Phys. Rev. Lett.* **2012**, *108*, 130503.
[81] S. L. Braunstein, S. Pirandola, *Phys. Rev. Lett.* **2012**, *108*, 130502.
[82] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, U. L. Andersen, *Nat. Photonics* **2015**, *9*, 397.
[83] Y. Fu, H.-L. Yin, T.-Y. Chen, Z.-B. Chen, *Phys. Rev. Lett.* **2015**, *114*, 090501.
[84] E. Diamanti, A. Leverrier, *Entropy* **2015**, *17*, 6072.
[85] I. Devetak, A. Winter, *Proc. R. Soc. A* **2005**, *461*.
[86] A. Leverrier, *Phys. Rev. Lett.* **2017**, *118*, 200501.
[87] F. Dupuis, O. Fawzi, R. Renner, arXiv:quant-ph/1607.01796, **2016**.
[88] R. König, R. Renner, *J. Math. Phys.* **2005**, *46*, 122108.
[89] J. Barrett, R. Colbeck, A. Kent, *Phys. Rev. Lett.* **2013**, *110*, 010503.
[90] J. Ribeiro, G. Murta, S. Wehner, *Phys. Rev. A* **2018**, *97*, 022307.
[91] J. Ribeiro, G. Murta, S. Wehner, *Phys. Rev. A* **2019**, *100*, 026302.
[92] T. Holz, D. Miller, H. Kampermann, D. Bruß, *Phys. Rev. A* **2019**, *100*, 026301.
[93] L. Masanes, S. Pironio, A. Acín, *Nat. Commun.* **2008**, *2*, 238.
[94] M. Navascues, S. Pironio, A. Acin, *Phys. Rev. Lett.* **2007**, *98*, 010401.
[95] M. Navascues, S. Pironio, A. Acin, *New J. Phys.* **2008**, *10*, 073013.
[96] T. Holz, H. Kampermann, D. Bruß, arXiv:quant-ph/1910.11360, **2019**.
[97] V. Scarani, N. Gisin, *Phys. Rev. Lett.* **2001**, *87*, 117901.
[98] V. Scarani, N. Gisin, *Phys. Rev. A* **2001**, *65*, 012311.
[99] R. Augusiak, P. Horodecki, *Phys. Rev. A* **2009**, *80*, 042307.
[100] K. Horodecki, M. Horodecki, P. Horodecki, J. Oppenheim, *Phys. Rev. Lett.* **2005**, *94*, 160502.
[101] K. Horodecki, M. Horodecki, P. Horodecki, J. Oppenheim, *IEEE Trans. Inf. Theory* **2009**, *55*, 1898.
[102] P. Horodecki, R. Augusiak, *Phys. Rev. A* **2006**, *74*, 010302.
[103] S. Das, S. Bäuml, M. Winczewski, K. Horodecki, arXiv:1912.03646, **2019**.
[104] M. Takeoka, E. Kaur, W. Roga, M. M. Wilde, arXiv:1912.10658, **2019**.
[105] S. Pirandola, arXiv:1912.11355, **2019**.
[106] G. Carrara, H. Kampermann, D. Bruß, G. Murta, arXiv:2007.11553, **2020**.
[107] D. Leibfried, E. Knill, S. Seidelin, J. Britton, R. B. Blakestad, J. Chiaverini, D. B. Hume, W. M. Itano, J. D. Jost, C. Langer, R. Ozeri, R. Reichle, D. J. Wineland, *Nature* **2005**, *438*, 639.
[108] H. Häffner, W. Hänsel, C. F. Roos, J. Benhelm, D. Chek-al kar, M. Chwalla, T. Körber, U. D. Rapol, M. Riebe, P. O. Schmidt, C. Becher, O. Gühne, W. Dür, R. Blatt, *Nature* **2005**, *438*, 643.
[109] T. Monz, P. Schindler, J. T. Barreiro, M. Chwalla, D. Nigg, W. A. Coish, M. Harlander, W. Haensel, M. Hennrich, R. Blatt, *Phys. Rev. Lett.* **2011**, *106*, 130506.
[110] J.-W. Pan, Z.-B. Chen, C.-Y. Lu, H. Weinfurter, A. Zeilinger, M. Żukowski, *Rev. Mod. Phys.* **2012**, *84*, 777.
[111] X.-C. Yao, T.-X. Wang, P. Xu, H. Lu, G.-S. Pan, X.-H. Bao, C.-Z. Peng, C.-Y. Lu, Y.-A. Chen, J.-W. Pan, *Nat. Photonics* **2012**, *6*, 225.
[112] X.-L. Wang, L.-K. Chen, W. Li, H.-L. Huang, C. Liu, C. Chen, Y.-H. Luo, Z.-E. Su, D. Wu, Z.-D. Li, H. Lu, Y. Hu, X. Jiang, C.-Z. Peng, L. Li, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, J.-W. Pan, *Phys. Rev. Lett.* **2016**, *117*, 210502.
[113] H.-S. Zhong, Y. Li, W. Li, L.-C. Peng, Z.-E. Su, Y. Hu, Y.-M. He, X. Ding, W. Zhang, H. Li, L. Zhang, Z. Wang, L. You, X.-L. Wang, X. Jiang, L. Li, Y.-A. Chen, N.-L. Liu, C.-Y. Lu, J.-W. Pan, *Phys. Rev. Lett.* **2018**, *121*, 250505.
[114] M. Malik, M. Erhard, M. Huber, M. Krenn, R. Fickler, A. Zeilinger, *Nat. Photonics* **2016**, *10*, 248.
[115] R. Barends, J. Kelly, A. Megrant, A. Veitia, D. Sank, E. Jeffrey, T. C. White, J. Mutus, A. G. Fowler, B. Campbell, Y. Chen, Z. Chen, B. Chiaro, A. Dunsworth, C. Neill, P. O'Malley, P. Roushan, A. Vainsencher, J. Wenner, A. N. Korotkov, A. N. Cleland, J. M. Martinis, *Nature* **2014**, *508*, 500.
[116] C. Song, K. Xu, W. Liu, C.-p. Yang, S.-B. Zheng, H. Deng, Q. Xie, K. Huang, Q. Guo, L. Zhang, P. Zhang, D. Xu, D. Zheng, X. Zhu, H.

Wang, Y.-A. Chen, C.-Y. Lu, S. Han, J.-W. Pan, *Phys. Rev. Lett.* **2017**, *119*, 180511.
[117] M. Gong, M.-C. Chen, Y. Zheng, S. Wang, C. Zha, H. Deng, Z. Yan, H. Rong, Y. Wu, S. Li, F. Chen, Y. Zhao, F. Liang, J. Lin, Y. Xu, C. Guo, L. Sun, A. D. Castellano, H. Wang, C. Peng, C.-Y. Lu, X. Zhu, J.-W. Pan, *Phys. Rev. Lett.* **2019**, *122*, 110501.
[118] S. B. van Dam, J. Cramer, T. H. Taminiau, R. Hanson, *Phys. Rev. Lett.* **2019**, *123*, 050401.
[119] L. Pezzè, A. Smerzi, M. K. Oberthaler, R. Schmied, P. Treutlein, *Rev. Mod. Phys.* **2018**, *90*, 035005.
[120] J. Ma, X. Wang, C. Sun, F. Nori, *Phys. Rep.* **2011**, *509*, 89.
[121] B. Lücke, J. Peise, G. Vitagliano, J. Arlt, L. Santos, G. Tóth, C. Klempt, *Phys. Rev. Lett.* **2014**, *112*, 155304.
[122] M. F. Riedel, P. Böhi, Y. Li, T. W. Hänsch, A. Sinatra, P. Treutlein, *Nature* **2010**, *464*, 1170.
[123] P. Kunkel, M. Prüfer, H. Strobel, D. Linnemann, A. Frölian, T. Gasenzer, M. Gärttner, M. K. Oberthaler, *Science* **2018**, *360*, 413.
[124] M. Fadel, T. Zibold, B. Décamps, P. Treutlein, *Science* **2018**, *360*, 409.
[125] K. Lange, J. Peise, B. Lücke, I. Kruse, G. Vitagliano, I. Apellaniz, M. Kleinmann, G. Tóth, C. Klempt, *Science* **2018**, *360*, 416.
[126] D. Dung, C. Kurtscheid, T. Damm, J. Schmitt, F. Vewinger, M. Weitz, J. Klaers, *Nat. Photonics* **2017**, *11*, 565.
[127] M. Proietti, J. Ho, F. Grasselli, P. Barrow, M. Malik, A. Fedrizzi, arXiv:quantum-ph/2002.01491, **2020**.
[128] L. Sheridan, V. Scarani, *Phys. Rev. A* **2010**, *82*, 030301.
[129] M. Pivoluska, M. Huber, M. Malik, *Phys. Rev. A* **2018**, *97*, 032312.

Glaucia Murta is currently a postdoc researcher at Heinrich-Heine-Universität Düsseldorf in Germany and member of the Cluster of Excellence "Matter and Light for Quantum Computing". She obtained her PhD from Federal University of Minas Gerais in Brazil and subsequently worked as postdoc researcher at QuTech-TU Delft in the Netherlands. Her research is focused on understanding how the properties of quantum systems can be used to design new and better protocols for cryptographic tasks.

Federico Grasselli is a young scientist specialized in quantum cryptography, a research field which promises to keep our data safe in the upcoming years. He received his education in Italy between Perugia (his hometown) and Milan, where he graduated with an MSc in Physics. He then completed his PhD in Physics at Heinrich-Heine-Universität Düsseldorf, Germany, where he is now working as a postdoc.

Hermann Kampermann is a Lecturer at Heinrich-Heine-Universität Düsseldorf, Germany. He received his PhD in 2004 from the University of Duisburg-Essen, Germany, and since the end of 2004 he is a member of the group of Dagmar Bruss at Heinrich-Heine-Universität Düsseldorf.

Dagmar Bruss obtained her PhD in theoretical particle physics from Universität Heidelberg, Germany, and spent some postdoc years in Oxford (UK), Turin (Italy) and Hannover (Germany). Since 2004 she is Head of the quantum information theory group at Heinrich-Heine-Universität Düsseldorf, Germany. She is interested in fundamental aspects of quantum information processing.