New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
15 April 2021

REVISED
2 July 2021

ACCEPTED FOR PUBLICATION
27 July 2021

PUBLISHED
12 August 2021

PAPER

Anonymous and secret communication in quantum networks

Christopher Thalacker[1,2], Frederik Hahn[3], Jarn de Jong[4], Anna Pappa[4] and Stefanie Barz[1,2,*]

[1] Institute for Functional Matter and Quantum Technologies, Universität Stuttgart, 70569 Stuttgart, Germany
[2] Center for Integrated Quantum Science and Technology (IQST), Universität Stuttgart, 70569 Stuttgart, Germany
[3] Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany
[4] Electrical Engineering and Computer Science Department, Technische Universität Berlin, 10587 Berlin, Germany
[*] Author to whom any correspondence should be addressed.

E-mail: barz@fmq.uni-stuttgart.de

Keywords: quantum communication, quantum networks, conference key agreement

Abstract

Secure communication is one of the key applications of quantum networks. In recent years, following the demands for identity protection in classical communication protocols, the need for anonymity has also emerged for quantum networks. Here, we demonstrate that quantum physics allows parties—besides communicating *securely* over a network—to also keep their *identities* secret. We implement such an anonymous quantum conference key agreement by sharing multipartite entangled states in a quantum network. We demonstrate the protocol with four parties and establish keys in subsets of the network—different combinations of two and three parties—whilst keeping the participating parties anonymous. We additionally show that the protocol is verifiable and run multiple key generation and verification routines. Our work thus addresses one of the key challenges of networked communication: keeping the identities of the communicating parties private.

Quantum communication has developed from first proof-of-principle demonstrations to real-world applications. Since the first proposals of using quantum physics to establish secret keys between two parties more than three decades ago [1–3], numerous demonstrations of quantum key distribution (QKD) have been performed. Starting from proof-of-concept experiments, intermediate and large-scale quantum networks spanning thousands of kilometres have recently been developed [4–10]. These experiments use single photons or entangled photon pairs to exchange a secret key between two parties and are known as QKD protocols [11, 12].

With growing complexity of quantum networks, new possibilities arise for multiparty protocols that go *beyond* bipartite secure communication. One example is *conference key agreement* (CKA), a cryptographic primitive that allows parties in a large-scale network to jointly establish a shared secret key [13]. Several approaches have been proposed with different requirements for quantum resources, ranging from bipartite to *multipartite* quantum states shared over the network. Interestingly, sharing multipartite states was shown to be more efficient in specific cases, e.g. for networks that have bottlenecks [14]. Recently, experimental implementations of CKA protocols have been performed [15].

Beyond the security of key generation, quantum networks open up a wide range of possibilities regarding other aspects of secure communication. One such aspect is *anonymity* [13, 15–18]. In a broad range of cases, internet users put much effort into keeping their activities and identities secret. As classical networks are replaced by their quantum counterparts, anonymity will likewise be a vital requirement for networked quantum communication.

Various levels of anonymity can be envisioned, and there exist multiple real-life scenarios where the identities of one or more of the communicating parties need to be kept secret. One example is whistle blowing, where it is imperative that the identity of the sender is kept secret. Combining anonymity with the

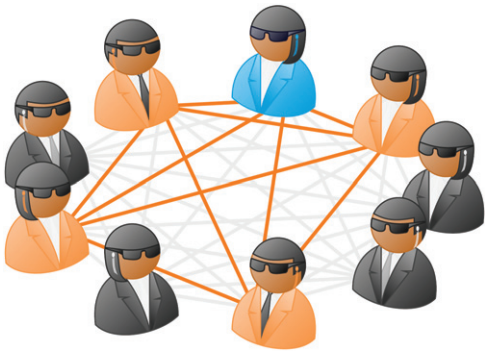


Figure 1. Anonymous conference key agreement. A sender (blue) aims to establish a secret key with m participants (orange) while their identities remain secret, both from each other and from the remaining non-participants (black).

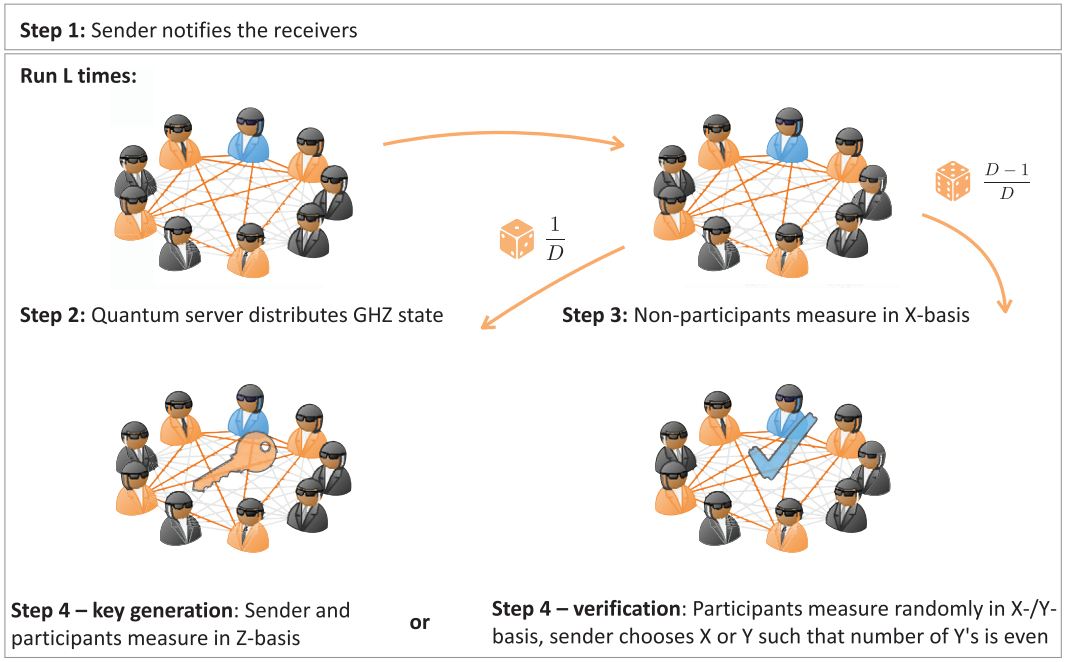
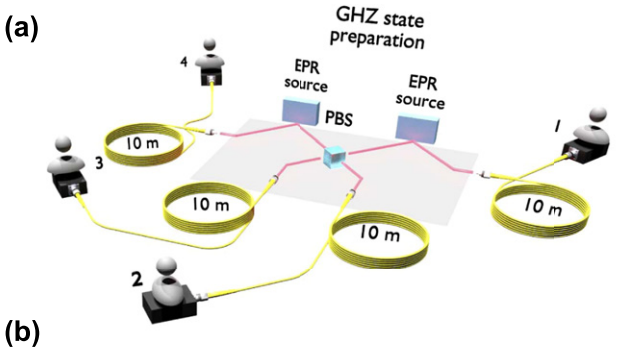


Figure 2. Sketch of the anonymous conference key agreement protocol. A sender (blue) notifies m participants (orange) and establishes a secret key. The identities of the participants remain secret from each other, and also from the remaining non-participants (black). See main text for detailed explanation of the protocol.

requirement for private communication between multiple parties leads to *anonymous conference key agreement* (ACKA) [16]. Here, the goal is to establish a secret key between several parties across a larger network in such a way that their identities are hidden from everyone else in the network, including each other, and are only known to the initiating party (see figure 1).

In this work, we demonstrate how to anonymously establish a secret key in a quantum network of four parties using multipartite entanglement. We focus on a protocol first proposed in [16], extending the work of [17, 19] on bipartite key generation.

Our protocol works as follows: first, each party is notified whether they are meant to participate in the key exchange or not [20]. Then, Greenberger–Horne–Zeilinger (GHZ) states are repeatedly shared with all parties in the network, such that each party receives one qubit from every shared state [21–25]. A few of these shared states are used to generate a secret key; the majority is used to detect an eavesdropper or any deviation of the parties from the protocol, making the protocol also *verifiable*. In our implementation, we demonstrate six different configurations for anonymously establishing a secret key between a sender and one or two participants in a four-partite network.



(c)

Configuration	KeyGen	Verification
A	$ZXZZ$	$XXXX, XXYY, YXYX, YXXY$
B	$XZZZ$	$XXXX, XXYY, XYYX, XYXY$
C	$ZZZX$	$XXXX, YYXX, YXYX, XYYX$
D	$ZZXZ$	$XXXX, XYXY, YXXY, YYXX$
E	$ZZXX$	$XXXX, YYXX$
F	$XXZZ$	$XXXX, XXYY$

Figure 3. The setting of our implementation. (a) Sketch of the experimental setup with four receivers. Two polarisation-encoded EPR photon pairs are generated and two photons—one of each pair—are superimposed on a PBS to generate a four-photon GHZ_4 state. This state is then distributed to the four parties. (b) Different network configurations implemented in our demonstration. The sender and the participants are highlighted in colour, while the non-participants are displayed in black. (c) Resulting measurement settings for each configuration and type of round, `KeyGen` or `verification`.

1. The protocol for anonymous conference key agreement

The goal of the protocol is for a sender to anonymously establish a key with m participants of their choice while they form part of a larger network of n parties. The network is able to distribute a state

$$|\mathrm{GHZ}_n\rangle := \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}\right) \tag{1}$$

between all n parties (cf figure 2).

The protocol starts with the n parties running a classical notification protocol that allows the sender to anonymously notify m participants—and thereby implicitly the non-participants [20]. This requires private classical communication between all pairs of parties. Once the participants are notified, the remainder of the protocol is repeated L times. In each round, a GHZ_n state is distributed to the n parties and the non-participants measure their qubits in the X-basis. This results in a GHZ_{m+1} state between only the sender and the participants, with an additional phase of ± 1 depending on the parity Δ of the measurement outcomes of the non-participants, i.e.

$$|\mathrm{GHZ}_{m+1,\Delta}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes(m+1)} + (-1)^{\Delta}|1\rangle^{\otimes(m+1)}\right). \tag{2}$$

In order for this phase to be compensated, the non-participants publicly announce their measurement outcomes—while the participants hide their identity by announcing random bits. The sender can tell

(a)

Configuration	#KeyGen	#Verification	D
A	2823	64379	23.8
B	1272	26056	21.5
C	1265	34924	28.6
D	2726	77484	29.4
E	2600	75298	30.0
F	2749	88202	33.1

(b)

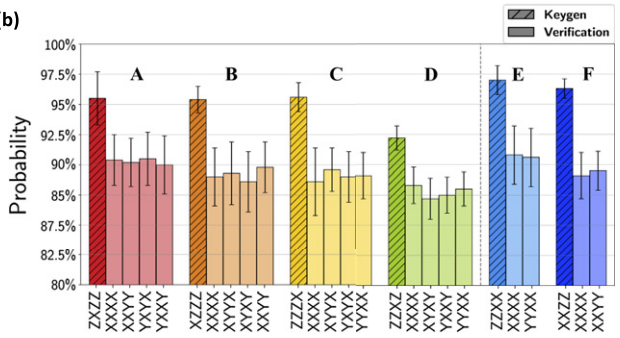


Figure 4. Experimental results. (a) Total number of `KeyGen` and `verification` rounds with corresponding security parameter $D = \frac{\texttt{\#Verification+\#KeyGen}}{\texttt{\#KeyGen}}$. (b) Success probability for key generation rounds (stripe pattern) and verification rounds (plain colour) for the different configurations. We calculate the probabilities per run; the error bars show the standard deviation over the number of runs.

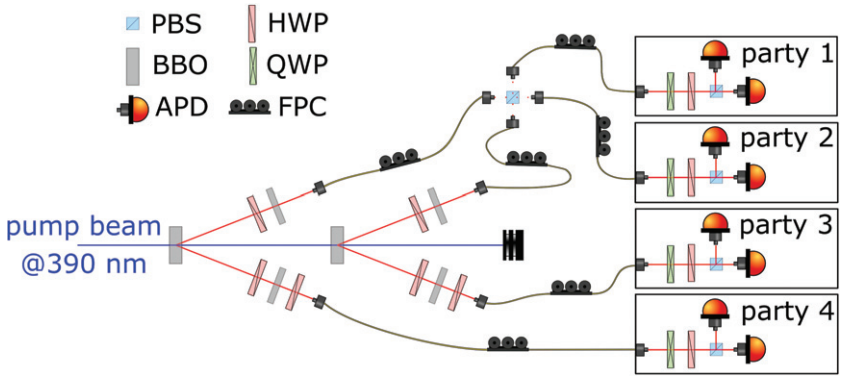


Figure 5. Experimental setup. Two β-barium borate (BBO) crystals are pumped with a fs-pulsed laser (390 nm) to generate polarisation-entangled photon pairs via type-II spontaneous parametric down-conversion. After passing a half-wave plate and an additional BBO, the photons are prepared in state $|\psi^-\rangle = (|H,V\rangle - |V,H\rangle)/\sqrt{2}$. Two photons, one from each source, are superimposed on a polarising beam splitter (PBS) to generate the four-photon state $|\mathrm{GHZ}\rangle = (|H,H,H,H\rangle + |V,V,V,V\rangle)/\sqrt{2}$ after postselecting four-photon events. The measurements as described in the main protocol are realised using quarter-wave (HWP) and half-wave plates (HWP), together with PBSs and avalanche photo detectors (APDs). FPC indicates fibre paddles for controlling the polarisation.

everyone apart and can now apply a local correction to her qubit, thereby canceling this phase. This allows the sender and the participants to anonymously 'extract' a smaller GHZ_{m+1} state shared only between themselves. This state can consequently be used to anonymously generate a shared secret key due to its inherent correlations when measured in the computational basis.

Note that, however, the non-participants could have diverged from their expected behaviour—for instance by not measuring their qubits and announcing instead a random bit. This would allow them to be part of the key-generating network, without being noticed. To prevent this, the participants use a large percentage of the shared GHZ_{m+1} states for anonymous verification. In these `verification` rounds, the participants perform measurements of random stabilisers on the GHZ_{m+1} state, whose outcome parity is known to be one. All participants announce their measurement bases and outcomes, while the non-participants announce two random bits concealing their roles. Only the sender is able to distinguish between these announcements and can thus validate the results. By performing $D-1$ randomly chosen `verification` rounds out of every D rounds in total, the sender can thus estimate the closeness of the distilled state to the ideal GHZ_{m+1} state [26]. This ensures that—even with arbitrary deviations from the protocol by the non-participants—the probability that the state is accepted despite being not close in trace distance to the GHZ state is small, as shown in [27]. It is therefore guaranteed that the resulting key is provably secure and secret, while also preserving anonymity as no communication takes place during the `KeyGen` rounds. We obtain a key of length L/D which is provably secure and the participants remain anonymous. Which of the rounds will be `verification` rounds and which `KeyGen` rounds is decided randomly with a bias such that $1/D$ rounds are used for verification.

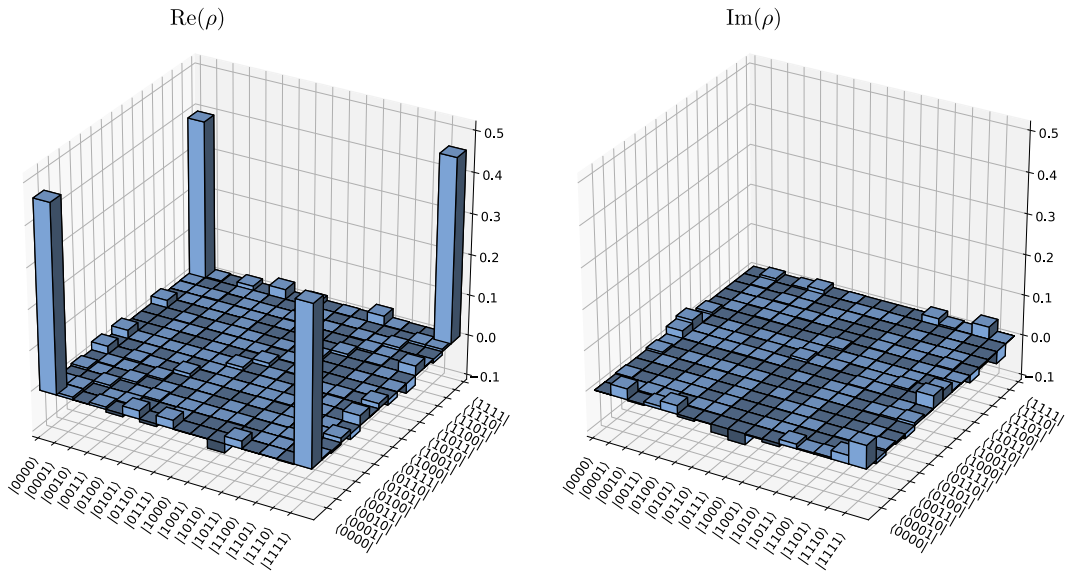


Figure 6. Reconstructed density matrix ρ of the GHZ_4 state used to implement the anonymous conference key agreement.

2. Experimental implementation

We demonstrate anonymous verifiable CKA in a network with four parties. We generate four-photon GHZ_4 states encoded in polarisation ($H = 0$, $V = 1$) using an all-optical setup as shown in figure 3(a) and in more detail in figure 5 in the appendix. The generated states have a fidelity of $F = 0.85(\pm 0.02)$, estimated via quantum state tomography [28].

The four-photon state allows us to demonstrate various configurations of the ACKA: a sender and two receivers, and a bipartite protocol with a sender and one receiver. In all configurations, as shown in figure 3(b), all participating parties remain anonymous. As a consequence, the non-participants do not know which and how many parties are in the end sharing a secret key, since they cannot distinguish between the different configurations.

We assume that the classical `notification` protocol has already been performed and we start by distributing the GHZ_4 states to all parties. First, the non-participants perform a measurement in the X-basis, resulting in a smaller GHZ_3 or GHZ_2 state.

We then randomly choose between `KeyGen` rounds and `verification` rounds. In a `KeyGen` round, all participants measure in the Z-basis and exploit the correlations of the GHZ state for establishing a shared key. In the `verification` rounds, each participant randomly measures in the X- or Y-basis and announces their basis together with their measurement outcome, while the sender announces random bits. Then, the sender performs either an X- or Y-measurement so that the total number of Y-measurements is even.

Figure 3(c) shows the different measurement configurations of each setting according to the protocol. In our implementation, all four measurements are implemented at the same time using motorised half-wave and quarter-wave plates, together with a polarising beam splitter.

For each configuration we run the protocol between 150 and 300 times, each run corresponding to a specific measurement setting. For each run, we integrate over 10 min of measurement time; each four-photon event is considered a round; this leads to the total number of `KeyGen` and `verification` rounds given in figure 4(a). Using these, we can calculate the effective security parameter $D = \frac{\texttt{\#Verification}+\texttt{\#KeyGen}}{\texttt{\#KeyGen}}$.

We estimate the probability of a correct `KeyGen` round and a passed `verification` for each run. We then calculate the averaged probabilities over all runs (see figure 4(b)) for all measurement operators and all implemented three-partite (**A**, **B**, **C** and **D**) and bipartite (**E** and **F**) network configurations. The success probability averaged over all the `KeyGen` runs is 95.3 with a standard deviation of $\pm 1.3\%$, whereas for the `verification` rounds the average success rate is $89.3(\pm 2.1)\%$.

The main source of noise in our implementation originates from higher-order emissions from the parametric down-conversion sources, which is about 3% of all four-fold coincidences at a pump power of 180 mW for each source. Furthermore, the generated Bell states show visibilities of about $\simeq 0.97$ when both qubits are measured in either the X- or the Z-basis. At the polarising beam splitter, we achieve two-photon

Configuration	Type of run	Basis	Number of runs	Total number of rounds	Number of successful rounds
A	KeyGen	$ZXZZ$	12	2823	2687
A	Verification	$XXXX$	67	15101	13635
A	Verification	$XXYY$	72	15548	14013
A	Verification	$YXYX$	72	16405	14825
A	Verification	$YXXY$	77	17325	15591
B	KeyGen	$XZZZ$	7	1272	1213
B	Verification	$XXXX$	46	1272	1213
B	Verification	$XYYX$	29	8322	7400
B	Verification	$XYXY$	36	5243	4680
B	Verification	$XXYY$	32	6084	5466
C	KeyGen	$ZZZX$	5	1265	1210
C	Verification	$XXXX$	39	9178	8134
C	Verification	$XYYX$	37	8778	7870
C	Verification	$YXYX$	35	8732	7773
C	Verification	$YYXX$	34	8236	7334
D	KeyGen	$ZZXZ$	5	2726	2515
D	Verification	$XXXX$	41	22321	19716
D	Verification	$XYXY$	41	21435	18683
D	Verification	$YXXY$	35	18772	16416
D	Verification	$YYXX$	28	14956	13162
E	KeyGen	$ZZXX$	14	2600	2521
E	Verification	$XXXX$	217	37141	33342
E	Verification	$YYXX$	219	38157	34157
F	KeyGen	$XXZZ$	9	2749	2647
F	Verification	$XXXX$	157	47136	42174
F	Verification	$XXYY$	134	41066	36873

Figure 7. List of all KeyGen and verification runs for each configuration. Each configuration has a certain set of measurement bases for KeyGen and verification. For each run, we integrate over 10 min of measurement time. The number of rounds refers to the total number of four-photon clicks in each basis, integrated over all runs. The number of successful rounds refers to the total number of four-photon clicks that correspond to a measurement result expected from the theory.

interference visibility of 0.823 ± 0.02, mainly limited through higher-order emissions, residual distinguishability of the photons, and, in particular, imperfect mode overlap.

As displayed in figure 4(a), the effective security parameter D ranges from about 20 to 32. If we just consider the number of verification rounds vs the number of KeyGen rounds, the probability $1/D$ of an adversary correctly guessing a round to be a KeyGen round is on average about 4% (see appendix). In that case they can perform a Z measurement instead of an X measurement. Thus, they would effectively take part in the KeyGen round and could compromise the security of the key. Note that this is the probability per individual key bit, and all key bits are uncorrelated in this regard.

In our implementation, the probability of a successful verification round is smaller than one. The worst-case scenario would be that all failed verification rounds are accepted, but are in fact caused by a malicious adversary actively cheating. Then, the adversary can cheat during all these failed verification rounds without being caught, thereby getting more 'tries' to cheat during the KeyGen rounds. In that case, the adversary has $\eta(D-1)$ of these extra attempts, where η is the *failure rate* of the verification rounds. The average probability of the adversary correctly guessing the KeyGen round becomes then $\frac{1+\eta(D-1)}{D}$. In our experiment, the adversary has a probability of $\sim$ 14% of correctly guessing each KeyGen round averaged over all different configurations (see appendix for individual values).

Configuration	No failed `Verification`	η	Worst-case	η'	Non-unit fidelity
A	0.042 (±8e-4)	0.097 (±0.011)	0.135 (±0.010)	0.019 (±0.015)	0.060 (±0.015)
B	0.047 (±0.0013)	0.108 (±0.012)	0.150 (±0.011)	0.030 (±0.016)	0.075 (±0.015)
C	0.035 (±0.001)	0.109 (±0.011)	0.140 (±0.011)	0.031 (±0.015)	0.065 (±0.015)
D	0.034 (±6e-4)	0.123 (±0.008)	0.152 (±0.007)	0.044 (±0.013)	0.077 (±0.013)
E	0.033 (±6e-4)	0.093 (±0.017)	0.123 (±0.016)	0.015 (±0.020)	0.048 (±0.019)
F	0.030 (±6e-4)	0.107 (±0.012)	0.134 (±0.012)	0.029 (±0.016)	0.058 (±0.016)
average	0.037 (±3e-4)	0.106 (±0.005)	0.139 (±0.005)	0.028 (±0.007)	0.064 (±0.006)

Figure 8. Probabilities for a potential adversary to correctly guess which round is the `KeyGen` round for each configuration and multiple scenarios. In the first scenario, corresponding to the second column ('no failed `verification`'), we assume the guessing probability is $\frac{1}{D}$. This means we consider the number of `verification` rounds vs `KeyGen` rounds, meaning that effectively no failed `verification` is allowed. The second scenario, corresponding to the fourth column ('worst case'), is a worst-case analysis, where all allowed `verification` failures (from our experimental results) are assumed to come from a malicious, cheating, adversary—such that the guessing probability becomes $\frac{1+\eta(D-1)}{D}$, where η is the failure rate of the `verification` rounds. The third and final scenario takes a more realistic approach ('non-unit fidelity'), where the non-unit fidelity of the shared GHZ_4 state is taken into account. Here, η is updated to η' to correct for the fact that some of the `verification` rounds will fail purely because of noise in the system—the updated guessing probability can be found in the sixth column. These are heuristic analyses, but the guessing probability p can be seen as (influencing) the information that the adversary possesses about the final raw key. These correlations with the adversary have to be deleted in post-processing, giving up a fraction $\sim h(p)$ of the raw key, where $h(p)$ is the binary entropy of p.

However, in reality, the fidelity of the GHZ_4 state is non-perfect, leading also to failed `verification` rounds. We can estimate the expected failure rate due to noise based on the (non-unit) fidelity of the distributed GHZ_4 state. We look for a lower bound on the expected failure rate so that the adversary has the maximum number of cheating attempts based on our fidelity. Using the trace distance and relating it to the fidelity, the lower bound on the expected failure rate can be estimated to be $r_f \geqslant 1 - \sqrt{F}$. We then replace η by $\eta' = \eta - r_f$, or 0 if this is negative. With this correction the probability of the adversary guessing the `KeyGen` round without being caught reduces to $\sim 7\%$ in our experiment (see appendix for more information).

In summary, our analysis shows that our `KeyGen` error rates are on average $< 5\%$ and are thus correctable using standard approaches. The probability of being correlated with the adversary can be bounded from above by $\lesssim 7\%$; additional correlations could be gained through error correction. Both contributions together are still expected to be within the limit that they can be reduced using privacy amplification [29]. Note that our arguments are meant to give an estimate of the viability of the experimental implementation and the subsequent post-processing steps. Performing these tasks in an anonymous fashion is a nontrivial task and further theoretical work is necessary to facilitate this.

Finally, we gather between 100 and 200 counts each run of 10 min integration time, which corresponds to 0.16–0.33 bps. Taking into account that 1/30 to 1/20 are `KeyGen` rounds and the rest is `verification` rounds, we get an effective keyrate between 0.006 and 0.017 bps. The classical post-processing necessary to obtain a perfectly secure key is, as mentioned before, out of the scope of this article, but it will affect the effective key rate.

3. Discussion

We have demonstrated how to anonymously and verifiably establish a shared key between several parties using multipartite quantum resources and exploiting the correlations of GHZ states. This is a significant step towards achieving secure and anonymous quantum communication, adding to the recent theoretical and experimental achievements in the field [13, 15–18].

For full-scale and real-life implementations of ACKA protocols, methods for error correction and privacy amplification need to be developed [30] and, also, finite key effects to be considered [15]. Even though we make a first attempt to quantify the effect of experimental imperfections on the security of the protocol, further research is still needed.

In this context, the effect of losses on general CKA has been studied recently [31]; it would be interesting to investigate whether a similar approach can be deployed while preserving anonymity. Future steps will be the implementation of our protocol in larger-scale networks and active switching for closing loopholes [32]. Finally, it will be interesting to see whether anonymity can be maintained with multipartite entangled resources other than GHZ states—and also, whether one can apply concepts like the one presented here to other quantum cryptographic primitives.

Acknowledgments

We thank Jelena Mackeprang and Lukas Rückle for comments, and Bülent Demirel for setting up the early stages of the experiment. AP and JdJ acknowledge support from the German Research Foundation (DFG, Emmy Noether Grant No. 418294583) and FH from the Studienstiftung des deutschen Volkes. CT and SB acknowledge support from the Carl Zeiss Foundation, the Centre for Integrated Quantum Science and Technology (IQ^{ST}), the German Research Foundation (DFG), the Federal Ministry of Education and Research (BMBF, project SiSiQ), and the Federal Ministry for Economic Affairs and Energy (BMWi, project PlanQK).

Data availability statement

The data that support the findings of this study are available upon reasonable request from the authors.

Appendix

Here, we give more information on the experimental setup for the implementation of the ACKA protocol. The experimental setup for the generation of the four-photon GHZ state is depicted and described in figure 5. Figure 6 depicts the reconstructed density matrix of the GHZ_4 state generated in the experiment. We also add more detailed information re the security parameters of our implementation. Figure 7 shows the number of runs and rounds we perform in our experiment. In figure 8 we list the values that an adversary correctly guesses a `KeyGen` round for each configuration, assuming an ideal state or a non-ideal state.

References

[1] Bennett C H and Brassard G 1984 *IEEE Int. Conf. Computers, Systems, and Signal Processing* pp 175–9
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Bennett C H, Bessette F, Brassard G, Salvail L and Smolin J 1992 *J. Cryptol.* **5** 3
[4] Ursin R *et al* 2007 *Nat. Phys.* **3** 481
[5] Peng C-Z *et al* 2007 *Phys. Rev. Lett.* **98** 010505
[6] Peev M *et al* 2009 *New J. Phys.* **11** 075001
[7] Sasaki M *et al* 2011 *Opt. Express* **19** 10387
[8] Liao S-K *et al* 2017 *Nature* **549** 43
[9] Pugh C J *et al* 2017 *Quantum Sci. Technol.* **2** 024009
[10] Chen Y-A *et al* 2021 *Nature* **589** 214
[11] Krenn M, Malik M, Scheidl T, Ursin R and Zeilinger A 2016 Quantum Communication with Photons *Optics in Our Time* vol 18 ed M Al-Amri, M El-Gomati and M Zubairy (Berlin: Springer) p 455
[12] Flamini F, Spagnolo N and Sciarrino F 2018 *Rep. Prog. Phys.* **82** 016001
[13] Murta G, Grasselli F, Kampermann H and Bruß D 2020 *Adv. Quantum Technol.* **3** 2000025
[14] Epping M, Kampermann H, Macchiavello C and Bruß D 2017 *New J. Phys.* **19** 093012
[15] Proietti M, Ho J, Grasselli F, Barrow P, Malik M and Fedrizzi A 2020 arXiv:2002.01491
[16] Hahn F, de Jong J and Pappa A 2020 *PRX Quantum* **1** 020325
[17] Unnikrishnan A, MacFarlane I J, Yi R, Diamanti E, Markham D and Kerenidis I 2019 *Phys. Rev. Lett.* **122** 240501
[18] Huang Z *et al* 2020 arXiv:2011.09480
[19] Yang Y-G, Yang Y-L, Lv X-L, Zhou Y-H and Shi W-M 2020 *Phys. Rev.* A **101** 062311
[20] Broadbent A and Tapp A 2007 *Advances in Cryptology—ASIACRYPT* (*Lecture Notes in Computer Science* vol 4833) ed K Kurosawa (Berlin: Springer) pp 410–26
[21] Greenberger D M, Horne M A and Zeilinger A 1989 *Bell's Theorem, Quantum Theory and Conceptions of the Universe* (Berlin: Springer) pp 69–72
[22] McCutcheon W *et al* 2016 *Nat. Commun.* **7** 13251
[23] Wang X-L *et al* 2016 *Phys. Rev. Lett.* **117** 210502
[24] Wang X-L *et al* 2018 *Phys. Rev. Lett.* **120** 260502
[25] Zhong H-S *et al* 2018 *Phys. Rev. Lett.* **121** 250505
[26] Pappa A, Chailloux A, Wehner S, Diamanti E and Kerenidis I 2012 *Phys. Rev. Lett.* **108** 260502
[27] Markham D and Krause A 2020 *Cryptography* **4** 3
[28] James D F V, Kwiat P G, Munro W J and White A G 2001 *Phys. Rev.* A **64** 052312

[29] Grasselli F 2021 *Quantum Cryptography* (Berlin: Springer) pp 55–70
[30] Grasselli F, Kampermann H and Bruß D 2019 *New J. Phys.* **21** 123002
[31] Singkanipa P and Kok P 2021 arXiv:2101.01483 [quant-ph]
[32] Huang A, Barz S, Andersson E and Makarov V 2018 *New J. Phys.* **20** 103016