npj | Quantum Information

www.nature.com/npjqi

ARTICLE OPEN

Experimental implementation of secure anonymous protocols on an eight-user quantum key distribution network

Zixin Huang[1,2,10✉], Siddarth Koduru Joshi[3,10✉], Djeylan Aktas[3,4], Cosmo Lupo[2,5], Armanda O. Quintavalle[2], Natarajan Venkatachalam[3], Sören Wengerowsky[6,7], Martin Lončarić[8], Sebastian Philipp Neumann[6], Bo Liu[9], Željko Samec[8], Laurent Kling[3], Mario Stipčević[8], Rupert Ursin[6] and John G. Rarity[3]

Anonymity in networked communication is vital for many privacy-preserving tasks. Secure key distribution alone is insufficient for high-security communications. Often, knowing who transmits a message to whom and when must also be kept hidden from an adversary. Here, we experimentally demonstrate five information-theoretically secure anonymity protocols on an eight user city-wide quantum network using polarisation entangled photon pairs. At the heart of these protocols is anonymous broadcasting, which is a cryptographic primitive that allows one user to reveal one bit of information while keeping their identity anonymous. For a network of n users, the protocols retain anonymity for the sender, given that no more than $n-2$ users are colluding. This is an implementation of genuine multi-user cryptographic protocols beyond standard QKD. Our anonymous protocols enhance the functionality of any fully-connected Quantum Key Distribution network without trusted nodes.

npj Quantum Information (2022)8:25 ; https://doi.org/10.1038/s41534-022-00535-1

INTRODUCTION

Quantum cryptography is one of the fastest-growing quantum technologies. Quantum Key Distribution (QKD) has been demonstrated across a huge spectrum of platforms[1,2], and proof-of-principle demonstrations are quickly being adapted into commercial prototypes. Recent experimental progress and the development of potentially large-scale networks[3–7] open up the possibility of a full-scale quantum internet[8–10]. Many protocols have been developed for multi-user quantum networks, such as secret voting[11,12], secret sharing[13,14], clock synchronisation[15], and distributed blind quantum computation[16]; these all use multipartite states. However, multipartite states are very complex to create and the performance of protocols based on such states can degrade rapidly with losses (i.e., distance). Protocols based on bipartite states, such as the ones presented here, are often the simplest and best choice given any realistic amount of loss. Further, they are compatible with today's state-of-the-art quantum networks, which distribute bipartite entanglement and use this to perform quantum communication.

As QKD matures as a technology, researchers turn their attention towards networked tasks beyond QKD, see, e.g., Refs. [17–24]. As we build the world's most secure networks, it is important to ensure that traffic on these networks is anonymous in addition to being impossible to decrypt. Thus, anonymity as a cryptographic primitive is becoming increasingly important for networked applications due to concerns for privacy and censorship. Applications include anonymous communication, secret auctions[25] and anonymous cryptocurrency transactions[26].

The first anonymous broadcating protocol was named the 'cryptographer's dining problem'[27]. There, n users establish shared secret keys with all the other users, allowing one (and only one) user to send a single bit of classical information whilst keeping their identity secret; we refer to this protocol as 'anonymous broadcasting'. Anonymous broadcasting is a particular case of a 'parity' protocol that allows n users to compute the parity of their local bit strings without revealing them. Later, Broadbent et al. derived a class of information-theoretically secure protocols based on the parity protocol that allows for practical anonymous communication to take place[28].

A traceless and efficient quantum anonymous broadcasting protocol was reported in Ref. [29]. There, a trusted resource distributes ahead of time an n-partite entangled GHZ (Greenberger-Horne-Zeilinger) state $|\psi\rangle_{\mathrm{GHZ}} = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}\right)$. While GHZ state-based networks are difficult to scale-up to many users, our approach exploits a scalable, fully connected, metropolitan-sized quantum network test bed[7].

The key enabler for the anonymity protocols in Ref. [28] is anonymous broadcasting, which requires pairwise shared secret keys between the users. In our setup, we use our quantum network to distribute pairwise secret keys between all the users, then perform secure anonymous protocols. While anonymous protocols can be achieved using classical cryptography primitives, the security of such protocols remains vulnerable to every form of attack that can compromise the classical keys used. By using quantum keys, we have upgraded the classical protocols to the general security assumptions of the underlying QKD protocol. Thus the QKD keys allow us to guarantee anonymity based on the fundamental laws of physics rather than computational complexity.

[1]Centre for Engineered Quantum Systems, Department of Physics and Astronomy, Macquarie University, Sydney, NSW 2109, Australia. [2]Department of Physics and Astronomy, The University of Sheffield, Sheffield S37RH, England. [3]Quantum Engineering Technology Labs, H. H. Wills Physics Laboratory & Department of Electrical and Electronic Engineering, University of Bristol, Bristol, England. [4]RCQI, Institute of Physics, Slovak Academy of Sciences, Dúbravská Cesta 9, 84511 Bratislava, Slovakia. [5]Dipartimento di Fisica, Politecnico di Bari, 70126 Bari, Italy. [6]Institute for Quantum Optics and Quantum Information - Vienna (IQOQI) & Vienna Center for Quantum Science and Technology (VCQ), Vienna, Austria. [7]Currently at ICFO-Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels, Barcelona, Spain. [8]Photonics and Quantum Optics Research Unit, Center of Excellence for Advanced Materials and Sensing Devices, Ruđer Bošković Institute, Zagreb, Croatia. [9]College of Advanced Interdisciplinary Studies, NUDT, Changsha 410073, China. [10]These authors contributed equally: Zixin Huang, Siddarth Kuduru Joshi. ✉email: zixin.huang@mq.edu.au; SKJoshi@Bristol.ac.uk

Published in partnership with The University of New South Wales

npj nature partner journals

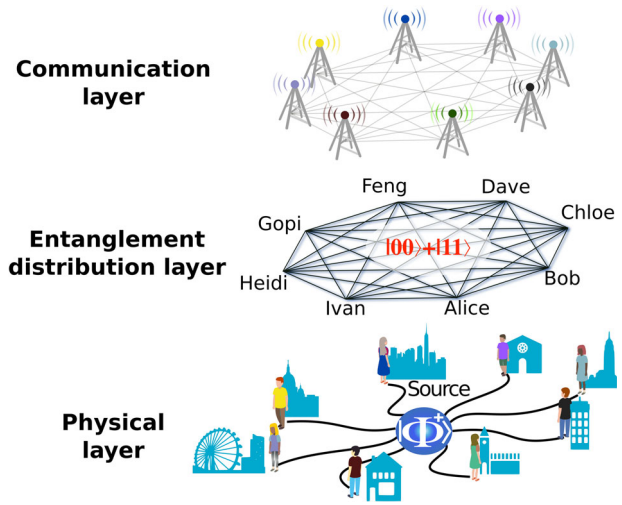

Fig. 1 Overview of the quantum network test bed. The physical layer consists of a broadband source of bipartite polarisation entanglement that is multiplexed and distributed to several users via one fibre each. In the entanglement distribution layer, polarisation entangled states are distributed to, and measured by each user. In the communication layer, they perform classical communication to generate the QKD keys, and execute the anonymous protocols described in this paper.

After obtaining keys from QKD, we solve the classical 'cryptographer's dining problem' and implement a number of practical communication protocols:

1. Anonymous broadcasting (parity) allows a single user to anonymously broadcast one bit of information.
2. Veto allows a single user to unilaterally stop or pass a binary decision-making task whilst remaining anonymous.
3. Notification: here, a user notifies a list of others but revealing neither the number of users nor their identity.
4. Collision detection is a protocol to verify whether there is a single sender or multiple senders.
5. Anonymous private message transmission allows a sender to anonymously transmit an encrypted message to a receiver, despite possible malicious interference from other users. The identities of both sender and receiver remain unknown to other users in the network.

The parity protocol (1) is derived in Ref. [27], and protocols 2–5 are proposed in Ref. [28]. Parity serves as a fundamental building block for the other protocols. Protocols 1–4 are combined to yield anonymous private message transmission (5).

The structure of the paper follows. In Section The Quantum Network, we introduce the quantum network we used to distribute unconditionally secure secret keys, and the experimental details are given in Section Methods. In Section Anonymous broadcasting (parity) to Anonymous private message transmission, we describe in detail the anonymous multi-user network protocols we executed using the quantum network. We present the communication rates in Section Communication rates.

RESULTS

The quantum network

The experiment was implemented using an eight-node city-scale quantum network based on bipartite entanglement distribution described in detail in Ref. [7]. Each of the eight users shares a different bipartite entangled state with every other user, forming the fully connected graph our protocols require. Furthermore, since every node directly shares entanglement with every other node, we do not make use of trusted nodes.

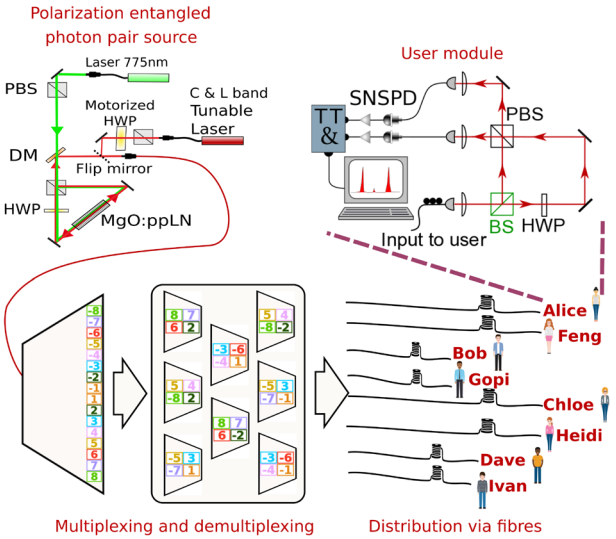

Fig. 2 Experimental setup. The entangled photon pair source is based on a type-0 MgO:ppLN crystal pumped bidirectionally by a 775.1 nm laser. A flip-mirror and motorised half wave plate (HWP) are used to couple a tunable telecom laser into the output fibre for polarisation control. The multiplexers/demultiplexers combine the shown combination of wavelength channels and distribute them to all eight users. The channel numbers are shown here plus 34 correspond to the standard ITU 100 GHz DWDM grid. Due to energy conservation photons in channels {1,−1}, {2,−2}, and so on are the only ones entangled. Each user is connected to the central hub by one fibre. The figure also shows the setup of each user's polarisation analysis and detection module. (PBS Polarisation beam splitter, DM Dichroic mirror, SNSPD Superconducting nanowire single photon detector, TT Time tagger, BS non-polarising Beam Splitter.

The network architecture can be understood as arising from the superposition of different layers, as shown in Fig. 1: (a) the physical layer consists of the hardware; (b) in the entanglement distribution layer, bipartite entanglement states are distributed and measured; (c) within the communication layer, users use authenticated classical communication channels to perform all the steps needed to generate QKD keys. The physical layer is shown in more detail in Fig. 2. It consists of the entanglement source, the multiplexers and demultiplexers needed to distribute the entanglement, a single transmission fibre for each user, and each user's detection module with the single photon detectors.

Each user measures all the photons they receive in either the horizontal/vertical (HV) or the diagonal/anti-diagonal (DA) polarisation basis. The modules to perform this measurement are shown in Fig. 2. Note that each user performs a passive basis choice using a 50:50 beam splitter and utilises just two detectors (rather than the typical four) by introducing a delay of 3.7 ns for detection events in the DA basis. Due to the distribution of photons and the measurements performed, every user now shares bipartite entanglement with every other user. This is depicted by the entanglement distribution layer (see Fig. 1).

In the communication layer, the above measurement outcomes are compared to generate a secret key following the BBM92 protocol[30] of QKD. To generate the secret keys, the users exchanged arrival time information. Since our network uses a unique two-detector measurement scheme (see Ref. [7] for implementation and security proof), the basis choice reconciliation information can be extracted from the temporal cross-correlation of the arrival time of photon detection events at any two users. For every user pair, these sifted keys are error corrected using a Low-Density Parity Check (LDPC) error correction code. Every user runs multiple instances of the key generation routine to generate keys from the sifted data. We used a security parameter of 10^{-5} for this

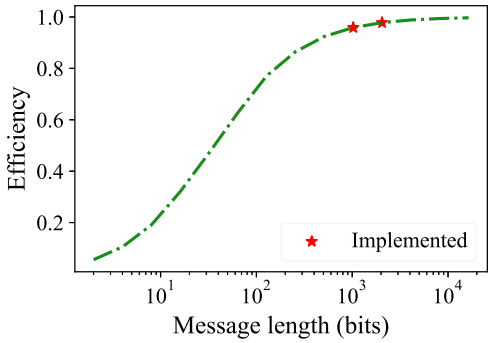

Fig. 3 Relationship between the protocols. A schematic that shows the dependence relationship between the protocols: anonymous broadcasting (parity) is the building block for all other protocols. The anonymous private message transmission requires collision detection, veto, and notification; collision detection is also made up of two veto protocols.

implementation users maintain a separate key store for every other user. The security and communication model assumptions follow from those of standard BBM92[30] protocol, taking into account the details of our particular implementation[7].

In summary, we use the quantum network for establishing secret keys between all users. To perform any of our anonymous protocols, users consume the desired number of bits from the appropriate key stores. Keys from the key stores are used only once.

Having established secure keys, the users can now perform multiple-party network protocols. As anticipated above, we perform five protocols: (1) anonymous broadcasting (parity), (2) veto, (3) notification, (4) collision detection, and (5) anonymous private message transmission. The relationship between the protocols is summarized in Fig. 3. The parity protocol (1) is the basic building block. All other protocols are based on it, adding more complexity and resilience against attacks. The veto protocol is instrumental for collision detection. The anonymous private message transmission is obtained by combining protocols 1–4 and represents our ultimate goal in this paper.

Anonymous broadcasting (parity)

The prerequisite of the anonymous broadcasting protocol is that each user holds a string of $n-1$ bits, in such a way that each pair of users shares a unique secret bit.

The goal of the protocol is for one of the user (called the speaker) to broadcast one bit of information to all other users anonymously. The assumption of the protocol is that there is only one speaker, and that at least two users are not colluding to guess the identity of the speaker. The classical communication protocol that achieves this goal is from Ref. [27] and is as follows:

1. If the speaker wishes to broadcast the bit value $c=0$, they do nothing. If, instead, they wish to broadcast the bit value $c=1$, then they flip one and only one of the $n-1$ bits in their local bit string.
2. Each user announces the modulo-two sum (i.e., the parity) of their local bit string.

Since every secret bit enters the addition modulo-two exactly twice, if no one transmits or if the transmitted bit is $c=0$, the parity of the outputs is also 0, otherwise it is equal to 1. In conclusion, the overall parity of the local strings, which is public, reveals the bit value c broadcast by the anonymous speaker.

Note that the purpose of the quantum network is to provide the unconditionally secure secret keys between each of the users, and the rest is classical. Each round of the anonymous broadcasting protocol consumes in total $n(n-1)/2$ secret bits. Ref. [27] provides an information-theoretic proof of the security of the anonymous broadcasting protocol, given that each user shares a private communication channel, i.e., a secure key with one another.

Anonymity: Intuitively, the protocol is anonymous for the following reasons: since a bit-flip is applied locally, no information transmission is necessary to change the overall parity. At the same time, the parity is a global feature and does not reveal the identity of the speaker.

Security: Some of the users may cooperate to uncover the identity of the speaker. If all $n-1$ users cooperate, then no protocol can keep the sender's identity secret. However, if there are t colluding users, then all other $n-t$ users are equally likely to be the sender.

What happens if there is more than one speaker? If more than one user flip their bit, this will lead to a collision error. Given that one speaker has sent the bit value $c=1$, let p be the probability that another speaker also wants to communicate the same bit value. An error in the overall parity value depends on having an odd or even number of additional speakers. The probability that i users want to communicate and $n-i-1$ do not is $^{pi}(1-p)^{n-i-1}$. Summing over odd values of i and overall permutations of the users, we obtain

$$P=\sum_{i\,\mathrm{odd}}^{n-1}\binom{n-1}{i}p^i(1-p)^{n-1-i}=\frac{1}{2}-\frac{1}{2}(1-2p)^{n-1}. \quad (1)$$

Collision errors become more problematic as the number of users becomes large. The collision detection protocol discussed in Subsection Collision detection addresses this issue.

Veto

The goal of this protocol is to allow the users to agree on a resolution unanimously, in such a way that if one or more users veto it, their identities remain undisclosed. Note that the parity protocol is unsuitable to achieve this goal. In fact, in the event of a collision with an even number of users transmitting the bit 1, the parity of the overall output will be 0.

Here, the aims of dishonest users would be to (1) uncover who has vetoed, (2) over turn the veto by attempting to set the overall parity to 0. Furthermore, (3) if the parity announcements are not simultaneous, the last user to announce their parity can always choose their input such that the overall parity is 0. The parity protocol ensures that (1) is not possible, (2) is addressed by introducing the auxiliary random variable c_i, and (3) is solved by changing the ordering of the users, as explained below.

To overcome these limitations, the users repeat the parity protocol βn times, for some integer $\beta>1$, that plays the role of a success probability parameter. For each implementation of the parity protocol, the order in which the users announce their local parity is changed, in such a way that each user has the opportunity to have the last word β times. Therefore, the prerequisite of the veto protocol is that each users pair shares βn secret random bits. This time it is allowed to have more than one speaker.

We assign to each user a binary variable. If the ith user chooses to veto, then $x_i=1$, otherwise $x_i=0$. The final output is 1 if at least one user submits the bit 1: therefore, the output of the veto protocol, when successful, is effectively the logical OR function of all of the x_i's, allowing all users to cast a vote.

The protocol is as follows[28]:

1. The n users agree on n orderings such that each ordering has a different last user. This step ensures that every user has a chance to be the last to broadcast. By changing the last user each round, the protocols ensure the last user cannot manipulate the result.
2. For each ordering, the following is repeated β times:

(a) Depending on x_i, each user sets the value of another binary variable, c_i, in the following way: if $x_i = 0$, then $c_i = 0$; otherwise if $x_i = 1$, then c_i is chosen randomly.
(b) The users execute the anonymous broadcasting protocol with inputs $\{c_i\}$. That is, if $c_i = 0$, they do nothing, and if $c_i = 1$, they flip the bit value of one of their modulo-two sum.
(c) If the parity at any round is 1, or if any user refuses to broadcast, then the result is set to 1 (implying a veto).

If for any of the β rounds the output is 1, then we know someone has vetoed. The value of c_i is randomly chosen to be either 0 or 1, so that if an even number of people want to veto, they do not end up with an even number of collisions all the time.

A single round of the veto protocol consumes $\beta n^2(n-1)/2$ secret bits and succeeds with probability at least $1 - 2^{-\beta}$. If all users in the protocol have $x_i = 0$, then the inputs to the anonymous broadcasting protocols are $c_i = 0$, then the output of the protocol is 0 with probability 1.

The protocol is designed such that a potential adversary is helpless to over turn the veto: suppose they want to set the output to be 0, then it is unfruitful for them to perform any action preemptively, since they do not know the value of the speaker's bit c_i.

Notification

The notification protocol allows any user to notify any other users, in such a way that the identities of both the notifier and the recipients remain secret, as well as the number of recipients. The notification protocol is essentially the veto protocol, except the potential recipient does not broadcast. It will be used as an intermediate step to achieve anonymous private message transmission.

For n users, each user has a n-bit string $(x_j^1, \ldots, x_j^n)$, where the index $j = 1, \ldots, n$ label the users. If user j wants to notify user i, he/she sets $x_j^i = 1$, and 0 otherwise. For each user i waiting to be notified, the following is repeated β times

1. Each user $j \neq i$ sets the value of another bit, c_j^i, in the following way: if $x_j^i = 0$, then $c_j^i = 0$; if $x_j^i = 1$, then c_j^i is chosen randomly.
2. The parity protocol is executed with inputs $c_1^i, c_2^i, \ldots, c_n^i$, with the exception that user i does not broadcast.
3. user i computes the overall parity in secret; he/she is notified if the parity is 1 for any run of the protocol.

Each round of the notification protocol consumes $\beta n^2(n-1)/2$ secret bits, and succeeds with probability at least $1 - 2^{-\beta}$.

Collision detection

As we have seen above, the parity protocol assumes that only one user wants to speak. Here we modify it in such a way that the protocol detects if more there is more than one speaker. Collision detection will be implemented as a part of anonymous private message transmission. The protocol is divided into two steps, A and B.

Step A is an application of the veto protocol. Each user who wants to speak inputs a bit value $x_i = 1$, or $x_i = 0$ otherwise. Note that if a user is a speaker, at the end of the veto protocol, they know (with high confidence if β is chosen large enough) if they are the only speaker. However, this information needs to remain private in order to protect the identity of the speaker.

Step B is a second run of the veto protocol. If during step A a speaker has detected the presence of another speaker, i.e., there was a collision, then they input the bit value $b_i = 1$. In this way, all the users will be notified of the collision.

The three outcomes for the collision detection protocol are:

$$\begin{cases} 0, & \text{if the output of A is 0} \\ 1, & \text{if the output of A is 1and the output of B is 0} \\ 2, & \text{if the output of A is 1and the output of B is 1.} \end{cases} \quad (2)$$

These correspond to no speaker, single speaker, and multiple speakers respectively. The collision detection protocol consumes at most $\beta n^2(n-1)$ secret bits, and succeeds with probability at least $(1 - 2^{-\beta})^2$.

Anonymous private message transmission

The anonymous private message transmission allows a sender to anonymously transmit an encrypted message to a receiver. To send an m-bit message, each user pair needs to share $(m + 2(\log\lceil m + 1\rceil + \beta)) + 4\beta n$ secret random bits with one another. The protocol first deals with potential collisions, verifying whether there is a single sender. Then the sender anonymously notifies the receiver (and only the receiver) that they are about to receive a message, followed by the message transmission. The message is encoded with an error detection code, which maps a m-bit string onto a $m' = m + 2\gamma$-bit string, where $\gamma < \beta + \log(m+1)$. The decoding process reveals whether the message has been tampered with, with success probability $1 - 2^{-\beta}$[31]. See Supplementary Material for details of the encoding and decoding. The protocol follows.

1. The users execute the collision detection protocol, and continue if there is a single sender.
2. Denote the unique sender as S and the receiver as R. The users perform the notification protocol, where S notifies that R is to receive a message.
3. The following message transmission protocol is executed:

(a) The sender encodes the message using an algebraic manipulation and detection code (see Supplementary Material), which maps the message M (of length m bits) into M', which has length $m' \approx m + 2(\log m + \beta)$ bits.
(b) The users perform m' rounds of the parity, where S uses M' as the input, R uses a random m'-bit string r as the input (a one-time pad), and all other users input 0 at every round.
(c) Let d be the output of the m' anonymous broadcasting protocol. The receiver computes $M'' = d \oplus r$.
(d) A veto protocol is performed. Everyone inputs 0 except for the receiver, who inputs 1 if an error is detected in the message, otherwise she inputs 0. If the output of veto is 1, this broadcasts to the sender that the message has been corrupted.

For anonymous private message transmission, we define the efficiency of the encoding as $m/(m + 2\gamma)$, which is the ratio of the message length to the required encoding. We plot $m/(m + 2\gamma)$ for $\beta = 16$ in Fig. 4. Evidently, the longer the input message, the more efficient the encoding becomes. For the experiment, we used two encodings. We map a 512 and 1024-bit message to a 554 and 1068-bit encoding, respectively, with $\gamma = 21$ (for the 512-bit message) and 22 (for the 1 kb message).

Ideally, we would like all protocols to be jamming-proof. However, the ideal functionality cannot always be achieved, since a single party can make the message transmission protocol abort. This is the price to pay to tolerate an arbitrary number of corrupt users and still provide information-theoretic privacy of the inputs[28].

Communication rates

We successfully implemented the five anonymous protocols on our quantum network testbed consisting of eight simultaneously

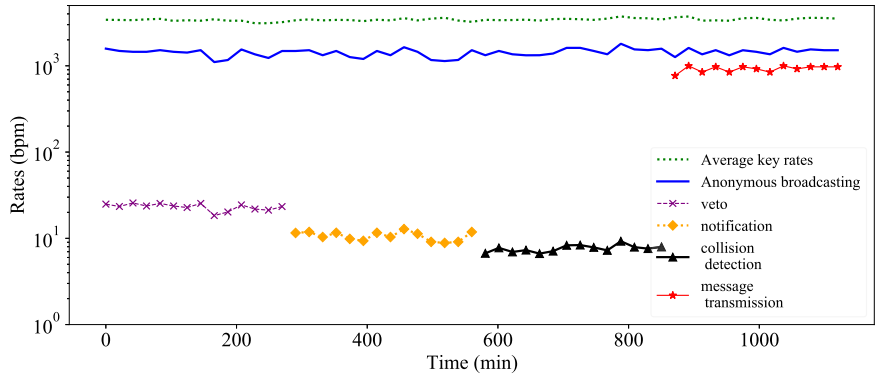

Fig. 4 Efficiency of the encoding. To encode a message of length m, the efficiency is $m/(m+2\gamma)$; we show this efficiency for different message lengths, given a fixed security parameter $\beta = 16$.

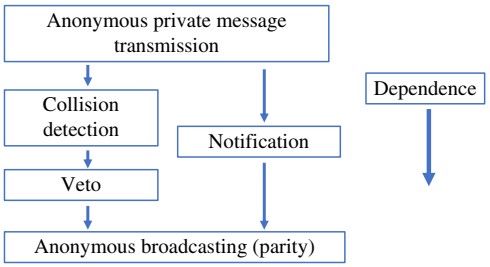

Fig. 5 Anonymous communication rates over time for the lab experiment. We show: the data the average key generation rate across all the links (green dotted line), anonymous broadcasting (parity) (blue solid line) and rate at which veto (purple crosses), notification (yellow diamonds), collision detection (black triangles) and message transmission (red stars) were performed. To ensure a minimum success probability of >99.99% (1 for veto) we used $\beta = 16$. Here the keys are generated every 20 min while including finite key effects.

connected users without trusted nodes. Our fully connected network, where every user exchanges secure keys with every other, is crucial to the implementation of these protocols. The superconducting detectors used provide roughly 18.4 h of continuous operation before the cryostats need to be thermally cycled. During this ~ 18 h run of the network, we chose to implement the basic anonymous broadcasting protocol throughout, then use this to implement the other four protocols one by one.

To demonstrate the stability of our network, we show the rate at which the protocols can be performed over the 18.4 h in Fig. 5. To be able to account for finite key effects with a security parameter of 10^{-5}, we generated the private keys once every 20 min. For each protocol, we use keys generated over a total time of 280 min. Due to the nature of the anonymous broadcasting protocol, the rate at which the protocol can be implemented is limited by the slowest link. This can be seen in the disparity between the average key rate and the anonymous broadcasting rate.

We implemented the veto protocol, for a random mixture of input 0 and 1's, likewise for the collision detection protocol. The veto protocol consumes the equivalent of only a few rounds of the anonymous broadcasting protocol if the input is 1, and βn rounds if the input is 0. The notification protocol consumes βn rounds regardless of the input. We believe that these protocols will prove to be useful for voting-based applications and truly private social media. Collision detection must become an important part of any anonymous network application. We believe that this could form the basis of a completely anonymous network control plane, which could optimally allocate resources and communication bandwidth without collecting individual users' network usage information.

For anonymous private message transmission, the protocol requires running an anonymous collision detection, veto and notification step. Thus the total number of bits consumed is larger. We executed the anonymous private message protocol using a mixture of 1 kb and 0.5 kb message lengths. The communication efficiency, which is the number of bits transmitted per parity protocol, is at least $m/(m + 2\log m + 2\beta + 4\beta n)$. The term of $4\beta n$ is due to the overheads associated with the sub-routines of collision detection, notification and veto protocols. This rate can be made arbitrarily close to 1 by choosing m large enough.

A summary of the number of secret bits consumed by each protocol is given in Table 1. We note that our protocols are tolerant to errors in the secure keys, and we discuss how in the Supplementary Material.

DISCUSSIONS

Quantum communication networks have largely focused on key distribution. Here, we have shown how these networks can be used to protect user privacy, a task often just as important as ensuring that a transmitted message is secure. In this work, we have implemented a set of five information-theoretically secure anonymous protocols – broadcasting, veto, notification, collision detection, and anonymous private message transmission on an eight-user quantum network. Since every user in the network shares a perfectly random, private and secure key with every other user, it becomes possible to implement these protocols. All the above protocols can be used as primitives for a wide range of applications.

We anticipate that the most useful protocol would be anonymous private message transmission, which allows one user to send an arbitrary-sized message to another user in secret. This has important implications for privacy-preserving applications, such as tipping off the police anonymously[26], secret voting, secure electronic auctions[25], and anonymous cryptocurrency transactions[32], multi-party computation[33] etc. Here we provide an explicit construction for the encoding and decoding of the message.

The above protocols only preserve anonymity within a single quantum network and their usefulness will grow as the size of the network increases. Maintaining anonymity in networks where active switching is used to choose which users can communicate at any given point in time or in scenarios where independent quantum networks are interconnected remains an open challenge.

We have used secret keys generated via QKD to perform protocols that allow for complete anonymity in a communication network. Our experiment represents quantum communications protocols beyond point-to-point QKD. It thus demonstrates the

Table 1. The number of secret bits and security parameters of protocols implemented in this paper. Here, n is the number of users and β is mutually agreed upon by all users to achieve a minimum desired success probability.

Protocol	No. of secret bits consumed	Success probability (minimum)
Parity	$n(n-1)/2$	1
Veto	$\beta n^2(n-1)/2$	$1-2^{-\beta}$
Notification	$\beta n^2(n-1)/2$	$1-2^{-\beta}$
Collision detection	$\beta n^2(n-1)$	$\left(1-2^{-\beta}\right)^2$
Message transmission (m-bit)	$(m+2(\log[m+1]+\beta))\times n(n-1)/2 + 2\beta n^2(n-1)$	$\left(1-2^{-\beta}\right)^5$

capabilities of a quantum network to realise non-trivial security tasks even when quantum memories are not available.

METHODS

Experimental setup

The entangled states are all produced by a single broadband source of polarisation entangled photon pairs. Polarisation entanglement is used to simplify each user's measurement module and is also compatible with long distance passively stable distribution over deployed fibres[34,35]. The output is de-multiplexed into 16 wavelength channels using International Telecommunications Union (ITU) 100 GHz top hat Dense Wavelength Division Multiplexing (DWDM) channels. The source itself is based on spontaneous parametric down-conversion of a 775.1 nm pump beam in a Magnesium oxide doped Periodically Poled Lithium Niobate (MgO:ppLN) crystal within a Sagnac interferometer, producing degenerate entangled photons centred at 1550.2 nm (which coincides with the 100 GHz (i.e.,0,8 nm) wide ITU channel Ch34 at 1550.12 nm) with a Full Width at Half Maximum bandwidth of ≈ 60 nm. Due to energy conservation during down-conversion, pairs are only found in channels at equal spectral distance from the central frequency. A 50-50 fibre beam splitter, attached to each DWDM channel, sends photons randomly to one of two output ports, which is equivalent to passive time division multiplexing. A multiplexing stage combines the channels together such that every user receives four frequency channels containing photons whose entangled partner photons were routed to four other users. The additional passive time division multiplexing due to the beam splitters expands the number of users in the network to eight, and ensures that every user shares entangled states with all seven other users.

DATA AVAILABILITY

All data from this publication is stored for at least 10 years on the University of Bristol's Research Data Storage Facility (RDSF). The processed data for the findings in this paper and programs to execute all protocols are available publicly from the RDSF, the raw data consisting of timetag files is too large to host publicly and available from the corresponding author (S.K.J.) on request.

Received: 24 November 2020; Accepted: 10 January 2022;
Published online: 07 March 2022

REFERENCES

1. Scarani, V. et al. The security of practical quantum key distribution. *Rev. Mod. Phys* **81**, 1301 (2009).
2. Pirandola, S. et al. Advances in quantum cryptography. *Adv. Opt* **12**, 1012 (2020).
3. Bradley, C. et al. A ten-qubit solid-state spin register with quantum memory up to one minute. *Phys. Rev. X* **9**, 031045 (2019).
4. Yin, J. et al. Satellite-based entanglement distribution over 1200 kilometers. *Science* **356**, 1140–1144 (2017).
5. Sun, Q.-C. et al. Quantum teleportation with independent sources and prior entanglement distribution over a network. *Nat. Photon* **10**, 671–675 (2016).
6. Wengerowsky, S., Joshi, S. K., Steinlechner, F., Hübel, H. & Ursin, R. An entanglement-based wavelength-multiplexed quantum communication network. *Nature* **564**, 225 (2018).
7. Joshi, S. K. et al. A trusted node–free eight-user metropolitan quantum communication network. *Sci. Adv.* **6**, eaba0959 (2020).
8. Wehner, S., Elkouss, D. & Hanson, R. Quantum internet: A vision for the road ahead. *Science* **362**, eaam9288 (2018).
9. Kimble, H. J. The quantum internet. *Nature* **453**, 1023–1030 (2008).
10. Li, G. Information Science & Technology in China: A Roadmap to 2050 (Springer, 2011).
11. Vaccaro, J. A., Spring, J. & Chefles, A. Quantum protocols for anonymous voting and surveying. *Phys. Rev. A* **75**, 012333 (2007).
12. Hillery, M., Ziman, M., Bužek, V. & Bieliková, M. Towards quantum-based privacy and voting. *Phys. Lett. A* **349**, 75–81 (2006).
13. Xiao, L., Long, G. L., Deng, F.-G. & Pan, J.-W. Efficient multiparty quantum-secret-sharing schemes. *Phys. Rev. A* **69**, 052307 (2004).
14. Hillery, M., Bužek, V. & Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **59**, 1829 (1999).
15. Komar, P. et al. A quantum network of clocks. *Nat. Phys* **10**, 582–587 (2014).
16. Beals, R. et al. Efficient distributed quantum computing. *Proc. Math. Phys. Eng. Sci.* **469**, 20120686 (2013).
17. Zhao, Z. et al. Experimental demonstration of five-photon entanglement and open-destination teleportation. *Nature* **430**, 54–58 (2004).
18. Yao, X.-C. et al. Observation of eight-photon entanglement. *Nat. Photon* **6**, 225–228 (2012).
19. Hahn, F., de Jong, J. & Pappa, A. Anonymous quantum conference key agreement. *PRX Quantum* **1**, 020325 (2020).
20. Hahn, F. et al. Anonymous conference key agreement in quantum networks. *Preprint at* https://arxiv.org/abs/2007.07995v1 (2020).
21. Pappa, A. et al. Experimental plug and play quantum coin flipping. *Nat. Commun* **5**, 1–8 (2014).
22. Solomons, N. R. et al. Scalable authentication and optimal flooding in a quantum network. Preprint at https://arxiv.org/abs/2101.12225v1 (2021).
23. Ng, N. H. Y., Joshi, S. K., Ming, C. C., Kurtsiefer, C. & Wehner, S. Experimental implementation of bit commitment in the noisy-storage model. *Nat. Commun* **3**, 1–7 (2012).
24. Zhou, H., Lv, K., Huang, L. & Ma, X. Security assessment and key management in a quantum network. *arXiv:1907.08963* (2019).
25. Stajano, F. & Anderson, R. The cocaine auction protocol: On the power of anonymous broadcast. In *International Workshop on Information Hiding*, 434–447 (Springer, 1999).
26. Menicucci, N. C., Baragiola, B. Q., Demarie, T. F. & Brennen, G. K. Anonymous broadcasting of classical information with a continuous-variable topological quantum code. *Phys. Rev. A* **97**, 032345 (2018).
27. Chaum, D. The dining cryptographers problem: Unconditional sender and recipient untraceability. *J. Cryptol.* **1**, 65–75 (1988).
28. Broadbent, A. & Tapp, A. Information-theoretic security without an honest majority. In *International Conference on the Theory and Application of Cryptology and Information Security*, 410–426 (Springer, 2007).
29. Christandl, M. & Wehner, S. *Advances in Cryptology–ASIACRYPT 2005, Proceedings* **3788**, 217–235 (2005).
30. Bennett, C. H., Brassard, G. & Mermin, N. D. Quantum cryptography without bell's theorem. *Phys. Rev. Lett.* **68**, 557 (1992).
31. Cramer, R., Dodis, Y., Fehr, S., Padró, C. & Wichs, D. Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 471–488 (Springer, 2008).
32. Ruffing, T., Moreno-Sanchez, P. & Kate, A. P2p mixing and unlinkable bitcoin transactions. In *NDSS*, 1–15 (2017).
33. Movahedi, M., Saia, J. & Zamani, M. Secure anonymous broadcast. Preprint at http://arXiv:1405.5326 (2014).
34. Wengerowsky, S. et al. Entanglement distribution over a 96-km-long submarine optical fiber. *PNAS* **116**, 6684–6688 (2019).
35. Wengerowsky, S. et al. Passively stable distribution of polarisation entanglement over 192 km of deployed optical fibre. *Npj Quantum Inf.* **6**, 1–5 (2020).

ACKNOWLEDGEMENTS

The research leading to this work has received funding from the Engineering and Physical Science Research Council (EPSRC) Quantum Communications Hubs EP/M013472/1 & EP/T001011/1 and equipment procured by the QuPIC project EP/N015126/1. Z.H. is supported by a Sydney Quantum Academy Fellowship. We acknowledge the Ministry of Science and Education (MSE) of Croatia, contract No. KK.01.1.1.01.0001. We acknowledge financial support from the Austrian Research

Promotion Agency (FFG) project ASAP12-85 and project SatNetQ 854022. This work was partially supported by the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement number 675662 (QCALL). The authors would also like to thank Peter P. Rohde for insightful discussions.

AUTHOR CONTRIBUTIONS

The theoretical aspects of this work was led by Z.H. with help from C.L. and A.O.Q. The experimental team was led by S.K.J. with D.A., S.W., M.L., S.P.N., Z.S., L.K., M.S., R.U. and J.G.R. Z.H. and S.K.J. contributed equally to this work. The software for processing the keys and implementing the algorithms was written by N.V., Z.H. and B.L. with help from S.K.J. The user modules were built by M.L., Z.S. and M.S., the source by S.W., S.P.N., S.K.J. and R.U. The multiplexing and distribution scheme was built by D.A. Funding for this work was obtained by J.G.R. with help from S.K.J. and D.A. S.K.J. coordinated the project. The paper was written by Z.H., S.K.J., D.A., C.L. and A.O.Q., the other authors proofread. All authors discussed the results and commented on the manuscript.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41534-022-00535-1.

Correspondence and requests for materials should be addressed to Zixin Huang or Siddarth Koduru Joshi.