Benchmarking of quantum protocols

Liao, Chin Te; Bahrani, Sima; da Silva, Francisco Ferreira; Kashefi, Elham

DOI
10.1038/s41598-022-08901-x

Publication date
2022

Document Version
Final published version

Published in
Scientific Reports

scientific reports

Check for updates

OPEN

Benchmarking of quantum protocols

Chin-Te Liao[1,7], Sima Bahrani[2,4,7]✉, Francisco Ferreira da Silva[5,6] & Elham Kashefi[1,2,3]

Quantum network protocols offer new functionalities such as enhanced security to communication and computational systems. Despite the rapid progress in quantum hardware, it has not yet reached a level of maturity that enables execution of many quantum protocols in practical settings. To develop quantum protocols in real world, it is necessary to examine their performance considering the imperfections in their practical implementation using simulation platforms. In this paper, we consider several quantum protocols that enable promising functionalities and services in near-future quantum networks. The protocols are chosen from both areas of quantum communication and quantum computation as follows: quantum money, W-state based anonymous transmission, verifiable blind quantum computation, and quantum digital signature. We use NetSquid simulation platform to evaluate the effect of various sources of noise on the performance of these protocols, considering different figures of merit. We find that to enable quantum money protocol, the decoherence time constant of the quantum memory must be at least three times the storage time of qubits. Furthermore, our simulation results for the w-state based anonymous transmission protocol show that to achieve an average fidelity above 0.8 in this protocol, the storage time of sender's and receiver's particles in the quantum memory must be less than half of the decoherence time constant of the quantum memory. We have also investigated the effect of gate imperfections on the performance of verifiable blind quantum computation. We find that with our chosen parameters, if the depolarizing probability of quantum gates is equal to or greater than 0.05, the security of the protocol cannot be guaranteed. Lastly, our simulation results for quantum digital signature protocol show that channel loss has a significant effect on the probability of repudiation.

In recent years, quantum technologies have seen significant advancements[1–4]. The rapid development in quantum hardware components such as single-photon detectors and quantum memories promises a vision of small-scale and large-scale quantum networks with real world applications[5–7]. Quantum networks offer new functionalities and services that are not possible in their classical counterpart. Prominent examples are secure communication and computation enabled by quantum cryptography, quantum secure direct communication (QSDC), blind quantum computing and distributed secure quantum machine learning[3,8–15]. Whereas quantum networks are not meant to replace existing classical ones, they have a great potential to extend the capabilities of classical networks.

Quantum protocols, as the use cases of quantum networks, offer unique communication and computation features. The most well-known example is quantum key distribution (QKD), which provides forward secrecy. Moreover, quantum cryptographic protocols such as quantum money and quantum digital signature (QDS) enable guaranteeing unforgeability with desired security level[16–20]. Another significant example is verifiable blind quantum computation (VBQC), which enables delegated quantum computation while preserving privacy[21,22]. Whereas the advantages offered by these protocols are promising, their commercial deployment requires several steps to be taken.

One major requirement in the development of quantum protocols in real world is the evaluation of their performance in various aspects such as security, required resources, and scalability. Such detailed performance analysis is required to include different sources of imperfection in the practical implementation. This type of benchmarking is mainly important due to the gap between the analyses provided by the academia community in the proposed theoretical protocols and the requirements recommended by experimentalists. Furthermore, it will provide us a tool to compare different quantum protocols with the same functionality proposed in the

[1]VeriQloud, Paris, France. [2]School of Informatics, University of Edinburgh, Edinburgh, UK. [3]CNRS, LIP6, Sorbonne Université, Paris, France. [4]High Performance Networks Group, Merchant Venturers Building, University of Bristol, Bristol, UK. [5]QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands. [6]Kavli Institute of Nanoscience, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands. [7]These authors contributed equally: Chin-Te Liao and Sima Bahrani. ✉email: si.bahrani@gmail.com

Protocol step	Major sources of noise and loss
Banknote preparation and transmission to user	Decoherence
	Transmission loss
Storage in quantum memory	Noise introduced by quantum memory
Measurement	Loss introduced by measurement
	Measurement error

Table 1. Major sources of noise and loss in quantum money protocol.

literature, e.g., different quantum token protocols. Such comparison is crucial in determining the commercial applications and use cases of quantum protocols.

Another prerequisite for commercial deployment of quantum protocols is to benchmark them against classical and post-quantum protocols with the same functionality. For instance, it would be desirable to compare QKD to symmetric key encryption methods in terms of security, required resources, scalability, and forward secrecy. Another significant example is quantum secure multi-party computation (SMPC)[23], and its benchmarking against classical SMPC. While this type of benchmarking is of paramount importance, it requires the data provided by the evaluation of quantum protocols in practical settings.

The two types of benchmarking mentioned above, are crucial prerequisites for designing quantum networks. Quantum networks require classical communication for various purposes such as synchronization and control messages. Besides, some quantum protocols, e.g., anonymous transmission, consist of intertwined quantum and classical sub-algorithms. Such integration of quantum and classical building blocks requires a detailed analysis of the interaction between them. In particular, any error or delay in classical communication may adversely affect the performance of quantum sub-algorithms. For instance, the delay in classical messages may increase the decoherence of quantum states in quantum memories. Therefore, to design quantum networks efficiently, it is necessary to determine the impact of classical messages/sub-algorithms involved in the quantum protocols.

One approach to benchmark quantum protocols is to investigate their performance considering fixed values for system parameters and desired figures of merit. This method will help us to evaluate the effect of specific protocol/hardware parameters and examine the feasibility of practical implementation considering currently achievable parameter values. Another method for benchmarking of quantum protocols is to consider target values for our desired figures of merit and determine the minimum requirements at the hardware level to achieve them. This method, previously proposed in[24], enables us to optimize system parameters and determine minimum viable requirements to achieve specific target values for figures of merit. We refer to this method as *backward benchmarking*. In this paper, we mainly focus on the first method of benchmarking. Nevertheless, we provide an example of backward benchmarking by adapting this method for quantum money protocol.

NetSquid is a software tool which provides a platform for simulating quantum networks and quantum computing systems[25]. This software enables simulation of quantum networks considering various aspects such as physical layer characteristics and control plane. The design of NetSquid is based on discrete-event simulation, which provides us a powerful tool to simulate the decoherence of quantum states by time and analyse the noise in quantum systems accurately. For instance, time-dependent noise affecting the quantum states stored in a quantum memory can be simulated effectively.

In this paper, we use NetSquid to simulate several quantum protocols and analyse their performance in the presence of various imperfections in the system. In the following sections, benchmarking of quantum money protocol, W-state based anonymous transmission, VBQC, and QDS are presented. Moreover, we provide an example of the backward benchmarking by applying this method to quantum money protocol.

Benchmarking of quantum money protocol

Private-key quantum money with classical verification enables a trusted bank to provide unforgeable banknotes to clients. Here, we consider the quantum money protocol proposed in[16]. The steps of the protocol are as follows:

(1) Bank randomly chooses n qubit pairs from the following set:

$$S_{pair} = \{|0+\rangle, |0-\rangle, |1+\rangle, |1-\rangle, |+0\rangle, |-0\rangle, |+1\rangle, |-1\rangle\}, \tag{1}$$

and sends them as banknote to the client.
(2) Client stores the received qubits in quantum memory.
(3) Client waits for T seconds. Then, she allows the verifier to access the banknote.
(4) The verifier randomly chooses between the two bases X and Z, and measures all $2n$ qubits in the chosen basis.
(5) Bank and verifier communicate via a classical channel and check the measurement outcomes. If the number of valid outcomes from the qubits in the chosen basis is larger than a predetermined threshold, bank verifies the validity of the banknote.

In a practical implementation of this protocol, various sources of loss and noise adversely affect the performance of the system. Table 1 shows major sources of loss and noise for this protocol.

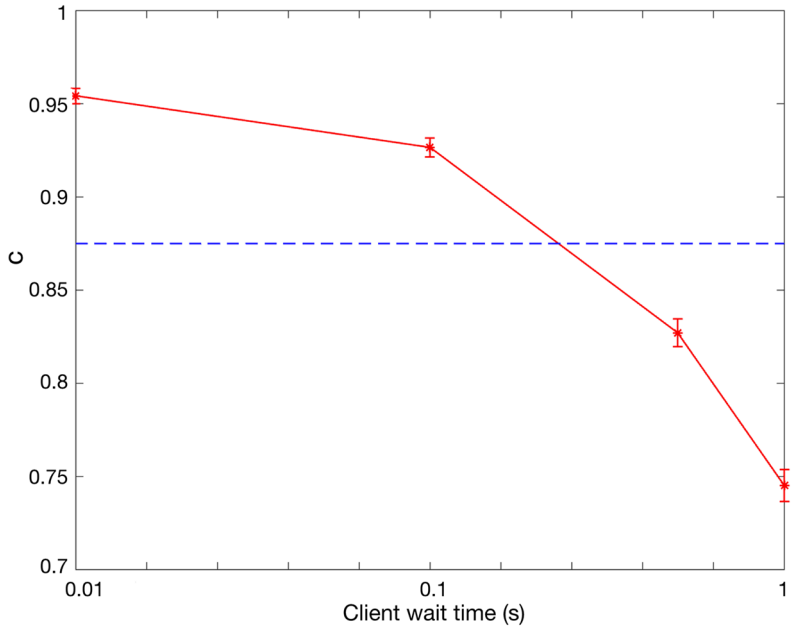

Figure 1. c versus client wait time, T. The blue dashed line shows the security threshold 0.875.

Figures of merit. *Probability of correctness.* One of the main figures of merit for this protocol is the probability of successful verification assuming an honest client. This parameter characterizes how system imperfections lead to rejection of the banknote in the verification phase wrongly. In[16], it has been shown that the lower bound for this parameter is given by

$$P_{\text{correct}} \geq 1 - e^{-cn\delta^2/2}, \tag{2}$$

where c is the probability of successful verification assuming an honest client, for mini-scheme quantum money protocol with just one qubit pair (for more details please refer to[16]). The parameter δ is defined as

$$\delta = \frac{2c}{3} - \frac{7}{12}. \tag{3}$$

It is worth noting that if $c > 0.875$ the security of the protocol can be guaranteed.

Probability of forge. Another figure of merit for this protocol is the probability of successful forging, e.g., duplication of the banknote by a dishonest client. An upper bound for this parameter is given by[16]

$$P_{\text{forge}} \leq e^{-n\delta^2/4}. \tag{4}$$

Simulation results. We use NetSquid to simulate the quantum money protocol explained above. In particular, our goal is to investigate the effect of quantum memory and measurement error on the performance of this protocol. Hence, we do not consider any source of loss. Simulation parameters are chosen based on currently achievable hardware parameters in nitrogen-vacancy (NV) center implementation. We assume T1T2 noise model with $T_1 = 10\,\text{h}$ and $T_2 = 1\,\text{s}$[25], where T_1 and T_2 denote the decay time constant of the quantum memory and the decoherence time constant of the quantum memory, respectively. Measurement error has been modelled with $p_1 = 0.05$ and $p_2 = 0.005$, where p_1 is the probability that a measurement result 0 is flipped to 1, and p_2 is the probability that a measurement result 1 is flipped to 0[25].

To evaluate the performance of the system, in the first step we obtain the parameter c by simulation. The parameter c is then used to calculate the security bounds for P_{correct} and P_{forge}. To obtain c by simulation, a block of 10,000 qubit pairs is sent and the simulation is repeated ten times to achieve better accuracy. The parameter c is then given by $N_{\text{valid}}/N_{\text{detected}}$, where N_{valid} is the number of valid outcomes corresponding to the qubits in the chosen basis, and N_{detected} denotes the number of detected outcomes corresponding to the qubits in the chosen basis.

Figure 1 shows c for different values of client wait time, T. The error bars corresponding to a confidence level of 95% are also shown in the figure. The blue dashed line shows the threshold 0.875. The parameter T characterizes any delay in the system before measuring the qubits; hence it is equal to the storage time of qubits in the quantum memory. Note that for a quantum memory with parameters T_1 and T_2, a longer storage time results in a higher decoherence noise and a lower c. It can be seen that for T larger than about 0.3 s the protocol is not guaranteed to be secure anymore. This value is about one third of $T_2 = 1\,\text{s}$. This shows that minimizing the

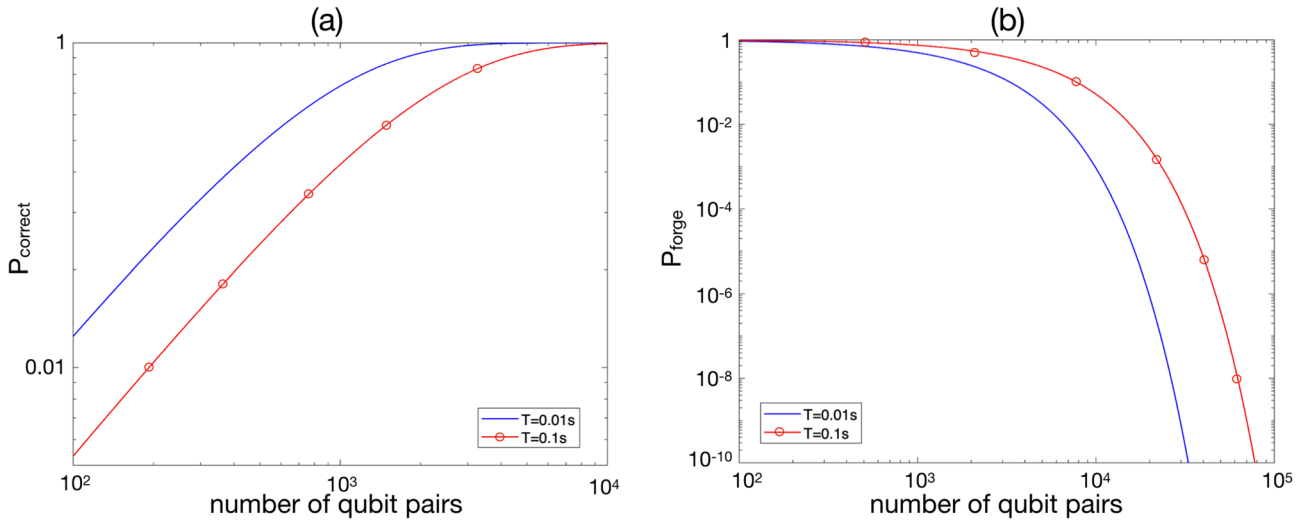

Figure 2. (**a**) P_{correct} versus number of qubit pairs for $T = 0.01$ s and $T = 0.1$ s. (**b**) P_{forge} versus number of qubit pairs for $T = 0.01$ s and $T = 0.1$ s.

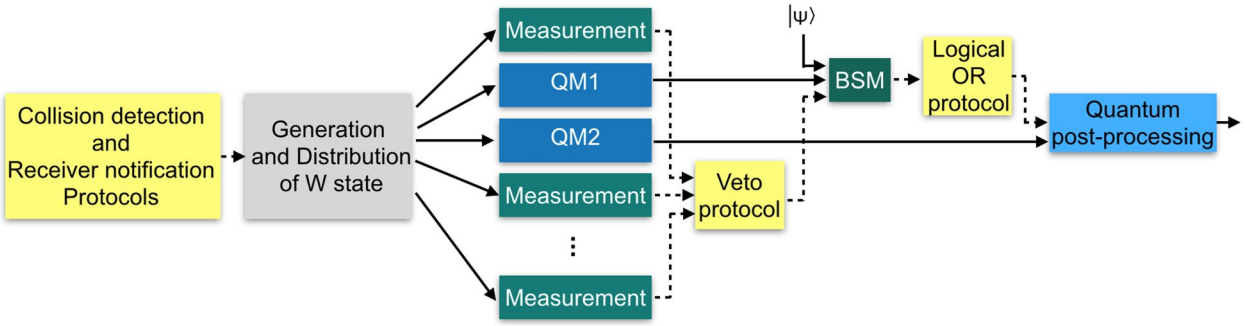

Figure 3. General description of W-state based anonymous transmission protocol. Solid arrows represent quantum communication, while dotted arrows represent classical communication. *QM* quantum memory, *BSM* Bell state measurement.

storage time of qubits in the quantum memory is crucial in the practical implementation of this protocol. In order to evaluate the required number of qubit pairs to achieve a specific security level, the parameters P_{correct} and P_{forge}, for $T = 0.01$ s and $T = 0.1$ s are shown in Fig. 2. According to Fig. 1, the security of the protocol is guaranteed in these two values of T. We consider the threshold 10^{-7} for P_{forge}. To achieve this threshold, the number of qubit pairs is required to be larger than about $n = 2.3 \times 10^4$ for $T = 0.01$ s, whereas for $T = 0.1$ s, the minimum required n increases to 5.4×10^4. This implies that the storage time of qubits has a huge effect on the minimum qubit pairs required to achieve a specific security level. For more details on NetSquid simulation for this protocol please refer to Appendix D (Supplementary Information).

Benchmarking of W-state based anonymous transmission

Anonymous transmission addresses the issue of concealing the identity of two communicating nodes in a quantum network with N nodes. More specifically, the identity of the sender S is required to be unknown to all other nodes in the network, whereas the identity of the receiver R is hidden to all other parties except the sender. In this section, we consider W-state based anonymous transmission protocol[26]. This protocol is mainly based on the establishment of anonymous entanglement between S and R. The entangled state between S and R is then used to teleport the desired state.

Figure 3 shows the general description of this protocol. At the first step, collision detection and receiver notification protocols[27] are used to determine a single sender S and notify the receiver R, respectively. Then, W state is generated and distributed among the users. In the next step, all users except for S and R perform measurement in the standard basis, while S and R keep their particles in the quantum memory. Measurement outcomes are, then, used in veto protocol[27], which determines whether all $N - 2$ outcomes are zero or not. In the latter case, the protocol aborts, while in the former case, it is assumed that anonymous entanglement is established between S and R. In that case, the protocol proceeds with the teleportation of the state $|\psi\rangle$. To this aim, S performs Bell state measurement and sends the two classical outcomes anonymously to R using logical OR protocol. The receiver R, then, uses this information to perform suitable quantum post-processing on his qubit.

Protocol step	Major sources of noise and loss
Generation and distribution of W state	Decoherence
	Transmission loss
Measurement performed by $N-2$ users	Loss introduced by measurement
Veto protocol	Noise introduced by quantum memory
	Loss introduced by quantum memory
Bell state measurement	Loss introduced by measurement
Anonymous transmission of two classical bits	Noise introduced by quantum memory
	Loss introduced by quantum memory
Quantum post-processing at receiver side	Noise introduced by quantum gates

Table 2. Major sources of noise and loss in anonymous transmission protocol.

To evaluate the performance of the protocol in the presence of system imperfections, it is necessary to consider major sources of loss and noise in the system, as summarized in Table 2. One major source of noise is the delay caused by classical sub-algorithms. During the run time of veto protocol, the particles of S and R are stored in the quantum memory, which introduces decoherence to the particles. Quantum memory noise also affects R's particle during the run time of logical OR protocol. Imperfect operation of quantum gates in the quantum post-processing step also introduces some noise in the system. Another source of noise is nonideal generation and distribution of W state, which is investigated in[26]. Aside from these nonidealities, losses in the system such as transmission loss (e.g. optical fibre loss) and the loss introduced by quantum memory may also adversely affect the performance of the protocol.

In the following, we consider several figures of merit for this protocol and investigate them in more details.

Figures of merit. *Probability of protocol failure.* W-state based anonymous transmission protocol is probabilistic[26], i.e., anonymous entanglement is established between S and R with some probability. Aside from that, losses in the system may cause the protocol to fail. In[26], it has been shown that this protocol tolerates one nonresponsive node among $N-2$ nodes (all nodes except S and R). Nevertheless, if S or R lose their particle, the protocol will fail. We can write the probability of protocol failure as follows:

$$\begin{aligned} P_{\text{fail}} = &(1 - Pr(D) + Pr(D)Pr(A|B))Pr(B) \\ &+ (1 - Pr(D) + Pr(D)Pr(A|C))Pr(C) \\ &+ (1 - Pr(B) - Pr(C)), \end{aligned} \tag{5}$$

where A is the event that at least one of measurement outcomes (inputs of veto protocol) is not zero, B is the event that all $N-2$ nodes that perform measurement are responsive, C is the event that just one out of $N-2$ nodes that perform measurement is nonresponsive, and D is the event that both S and R does not lose their particle. The probability $Pr(B)$ can be obtained by

$$Pr(B) = \prod_{\substack{i\in\{1,\ldots,N\} \\ i\neq i_S,i_R}} \eta_i, \tag{6}$$

where η_i is the transmittance corresponding to the ith node. Similarly, the probability $Pr(C)$ can be expressed as

$$Pr(C) = \sum_{i=1,i\neq i_S,i_R}^{N} \{(1-\eta_i) \prod_{\substack{j\in\{1,\ldots,N\} \\ j\neq i_S,i_R,i}} \eta_j\}. \tag{7}$$

The parameter $Pr(D)$ is given by

$$Pr(D) = \eta_{\text{BSM}}\eta_{i_S}\eta_{i_R}, \tag{8}$$

where η_{BSM} denotes the loss introduced by Bell state measurement. The probabilities $Pr(A|B)$ and $Pr(A|C)$ are calculated in Appendix A (Supplementary Information).

Probability of correctness. Probability of correctness is defined as the probability of successful teleportation of the state $|\psi\rangle$, under the assumption that all participants are honest and the protocol does not fail. We can write this parameter as follows:

$$P_{\text{correct}} = (1 - \varepsilon_{\text{corr}}). \tag{9}$$

In the above equation, $\varepsilon_{\text{corr}}$ represents the probability of failure in classical subroutines[26].

Fidelity of anonymous entanglement between S and R. The fidelity of the entangled state established between S and R is another important figure of merit for this protocol. This parameter is defined as

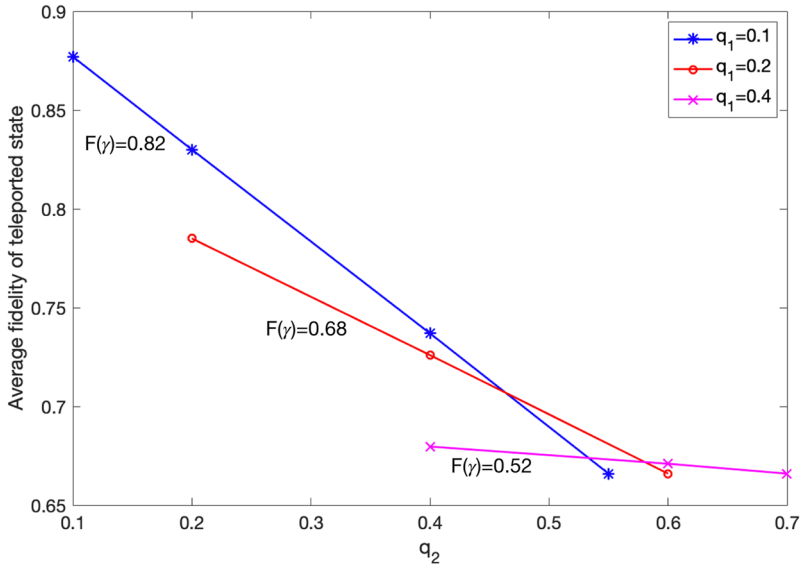

Figure 4. Average fidelity of the teleported state for different values of q_1 and q_2.

$$F(\gamma) = Tr[\gamma.\left|\Psi^+\right\rangle\left\langle\Psi^+\right|], \tag{10}$$

where γ is the anonymous entangled state between S and R and $\left|\Psi^+\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$.

Average fidelity of the teleported state. The goal of anonymous transmission protocol is to transmit a quantum state anonymously. Therefore, one of the most important figure of merits is the quality of the teleported state, which can be characterized by average fidelity. We write the quantum state to be teleported as a Bloch vector in Bloch sphere as follows:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)e^{i\phi/2}|0\rangle + \sin\left(\frac{\theta}{2}\right)e^{-i\phi/2}|1\rangle, \tag{11}$$

where θ and ϕ denote the polar and azimuthal angles, respectively. The average fidelity of the teleported state is given by[28]

$$F_{\text{ave}} = \frac{1}{4\pi}\int_0^{\pi} d\theta \int_0^{2\pi} F(\theta,\phi)\sin(\theta)d\phi, \tag{12}$$

where

$$F(\theta,\phi) = \text{Tr}[|\psi\rangle\langle\psi|\rho_{out}] \tag{13}$$

In the above equation, ρ_{out} denotes the density matrix for the teleported state corresponding to $|\psi\rangle$.

Simulation results. In this section, we present some simulation results for anonymous transmission protocol. We use NetSquid to simulate this protocol for four users. The average fidelity of the teleported state (Eq. (12)) is approximated using Reimann sum as follows:

$$F_{\text{ave}} \simeq \frac{\pi}{2\times 6400}\sum_{k=0}^{79}\sum_{m=0}^{79} g(\theta_k,\phi_m), \tag{14}$$

where $\theta_k = \frac{\pi}{160} + k\frac{\pi}{80}$, and $\phi_m = \frac{\pi}{80} + m\frac{2\pi}{80}$, for $k = 0, 1, 2, \ldots, 79$ and $m = 0, 1, 2, \ldots, 79$.

First of all, the effect of the noise introduced by quantum memories on the quality of the teleported state is evaluated. We assume that the particles of S and R are stored for the time duration of t_1 before teleportation. R's particle is assumed to be kept in the quantum memory for an additional time interval of t_2, i.e., total storage time for R's particle is $t_1 + t_2$. We consider dephasing noise model for quantum memories. The dephasing probabilities for S's and R's quantum memories are denoted by q_1 and q_2, respectively. The parameters q_1 and q_2 correspond to t_1 and $t_1 + t_2$, respectively.

Figure 4 shows F_{ave} for different values of q_1 and q_2. The fidelity of the anonymous entangled state, $F(\gamma)$, corresponding to each value of q_1 is also obtained by[26]

$$F(\gamma) = 1 - 2q_1(1 - q_1), \tag{15}$$

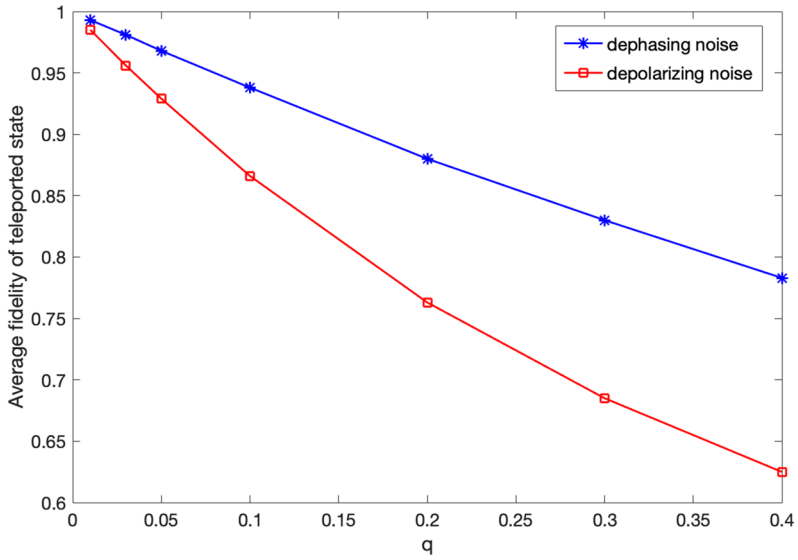

Figure 5. Average fidelity of the teleported state versus q.

and shown in Fig. 4. It can be seen that for $q_1 = 0.2$, the average fidelity of teleported state is already less than 0.8. With the assumption of $q_1 = (1 - e^{-t_1/T_2})/2$, where T_2 is the decoherence time constant of the quantum memory, this value corresponds to $t_1/T_2 = 0.51$. This implies that it is crucial to minimize the delay caused by veto protocol as much as possible.

It is worth noting that if $q_2 = q_1$, there is no noise after Bell state measurement. In this case, we can analytically calculate F_{ave} from $F(\gamma)$ using the formula $F_{\text{ave}} = (2F(\gamma) + 1)/3$[29]. It can simply be concluded that the analytical results obtained by this formula validates the simulations results for the cases $q_2 = q_1$ in Fig. 4.

Next, we evaluate the performance of the protocol in the presence of noise at the X and Z gates in the final step of the teleportation. We consider two noise models, dephasing and depolarizing, with dephasing/depolarizing probability denoted by q. Figure 5 shows F_{ave} versus q. It can be seen that the average fidelity of the teleported state in case of dephasing noise model is significantly higher than that of depolarizing noise model, especially for large values of q. As an example, in case of dephasing noise, for q smaller than about 0.15, F_{ave} is above 0.9, whereas in case of depolarizing noise we achieve this performance for q smaller than about 0.075. It is worth noting that the results presented in this section are independent of the number of users, N, since the sources of noise after measurement by all users except S and R are considered. For more details on NetSquid simulation for this protocol please refer to Appendix D (Supplementary Information).

Lastly, we present a numerical example to examine the effect of sources of loss in the system on the probability of protocol failure. We assume $\eta_{\text{d}} = \eta_{\text{BSM}} = 0.8$, where η_{d} denotes the measurement loss for each of $N - 2$ users. The transmittance corresponding to ith node (except S and R is, then, assumed to be $\eta_i = \eta_{\text{d}}\eta_{\text{tr}}$), where η_{tr} represents transmission loss. The loss introduced by quantum memories is modelled by $\eta_{\text{qm}} = \eta_0 e^{-t_s/T_1}$. Here, T_1 denotes decay time constant of quantum memory, t_s denotes the storage time, and η_0 is a constant less than one. The parameter η_0 is assumed to be 0.8. The ratio t_s/T_1 is assumed to be 0.002 for sender, and 0.004 for receiver.

Figure 6 shows the probability of protocol failure versus transmission loss for different values of N. It can be seen that the probability of protocol failure increases with the increase of number of users. For $N = 4$, this probability reaches one for transmission of loss about 10 dB. This value reduces to about 8 dB and 5.5 dB for 6 and 8 users, respectively.

In Appendix A (Supplementary Information), two cases of ideal W state and noisy W state with dephasing noise model are considered. It has been shown that dephasing noise does not change the probabilities $Pr(A|B)$ and $Pr(A|C)$ in (5) compared to that of noiseless case. Hence, the presented results in Fig. 6 are applicable to noisy W state with dephasing noise model as well.

Benchmarking of verifiable blind quantum computation

VBQC enables delegating quantum computation to a quantum server while preserving privacy[30]. In this paper, we choose the measurement-based VBQC protocol proposed in[30]. The steps of the protocol are outlined in Appendix B (Supplementary Information). We assume that three qubits are used at the server side. This protocol consists of d computation runs and t test runs. If the number of failed test runs is larger than a threshold denoted by w, the protocol aborts.

The main sources of noise in this protocol are imperfect operation of quantum gates and measurement errors. Aside from that, classical communication between client and server may introduce some delay, which substantially causes decoherence. Lastly, transmission loss may be troublesome, depending on the distance between client and server. In the following, two figures of merit for this protocol are presented.

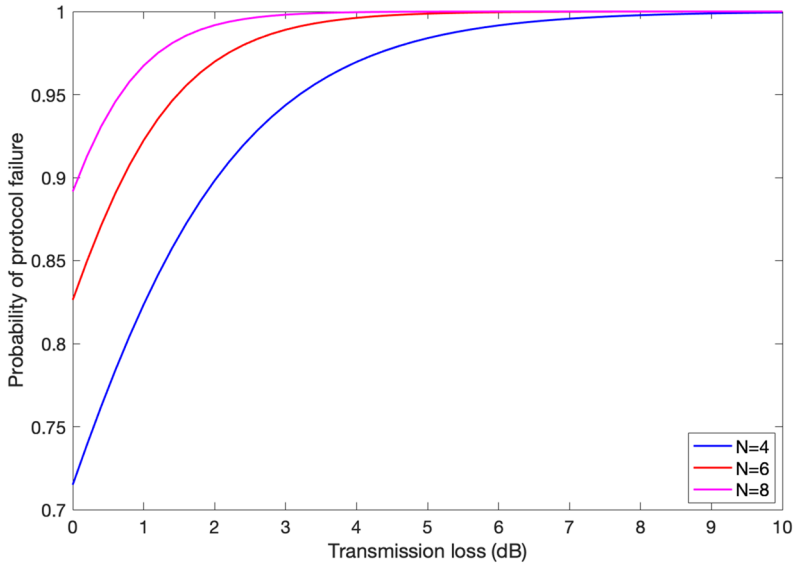

Figure 6. Probability of protocol failure versus transmission loss for different number of users.

	Duration
Single-qubit gate	5 ns
CNOT gate	20 μs
Control Z gate	20 μs
Measurement	3.7 μs

Table 3. Time duration of gates used in VBQC protocol.

Figures of merit. The probability of aborting assuming an honest server is one of the main figure of merits for this protocol. Suitable choice of protocol parameters such as w and t plays an important role in avoiding unnecessary aborting of the protocol while maintaining the security.

Another figure of merit for this protocol is probability of correctness, which is defined as the probability of correct output assuming the protocol does not abort.

Simulation results. In this subsection, we examine the performance of VBQC protocol in the presence of system imperfections. We use NetSquid to simulate the VBQC protocol outlined in Appendix B (Supplementary Information). We assume that the server has three qubits. Nominal values used for time duration of gates are listed in Table 3. These parameters are chosen based on the NV platform implementation[25]. We assume depolarizing noise model for the quantum gates. In our simulation, we assume that the depolarizing probability in quantum gates are identical. This provides us a benchmark for the performance of the protocol. As for measurement error, we use the bit flip model used in[25]. We assume that the measurement outcome 0 is flipped to 1 with probability 0.05, whereas the measurement outcome 1 is flipped to 0 with probability 0.005.

First of all, we evaluate the performance of a test run. We consider different values for depolarizing probability in quantum gates. In each case, the test run is performed for 3000 times and the probability of failure of a test run is calculated, as shown in Fig. 7. The upper and lower bounds for this probability, denoted by $P_{\max}$ and $P_{\min}$, respectively, depend on the desired confidence level. Here, the results for two confidence levels 95% and 99.95% are shown in Fig. 7.

We use the obtained values for $P_{\max}$ and $P_{\min}$ to determine the suitable range of values for w/t. In[30], it has been shown that if $w/t > P_{\max}$, the protocol is ε_c-locally-correct with exponentially low ε_c, i.e., with honest parties the output will be the expected one. On the other hand, according to[30], in order for the protocol to be secure, w/t should be less than $1/2k$, where k is the number of colouring in the protocol (for more information please refer to[30]). In our simulated protocol with a three-qubit server, $k = 2$. Hence, we have $P_{\max} < w/t < 0.25$. The threshold $1/2k = 0.25$ is shown in Fig. 7 by the blue dashed line. It can be seen from Fig. 7 that with our chosen parameters, for a depolarizing probability of 0.05, there is no acceptable value for w/t. If the depolarization probability is reduced to 0.03, it is feasible to choose parameter values satisfying $P_{\max} < w/t < 0.25$. Nevertheless, there are limited acceptable values for parameters w and t. To extend the range of acceptable parameter values and have more flexibility in choice of protocol parameters, it is necessary to enhance the depolarization probability of quantum gates beyond 0.03.

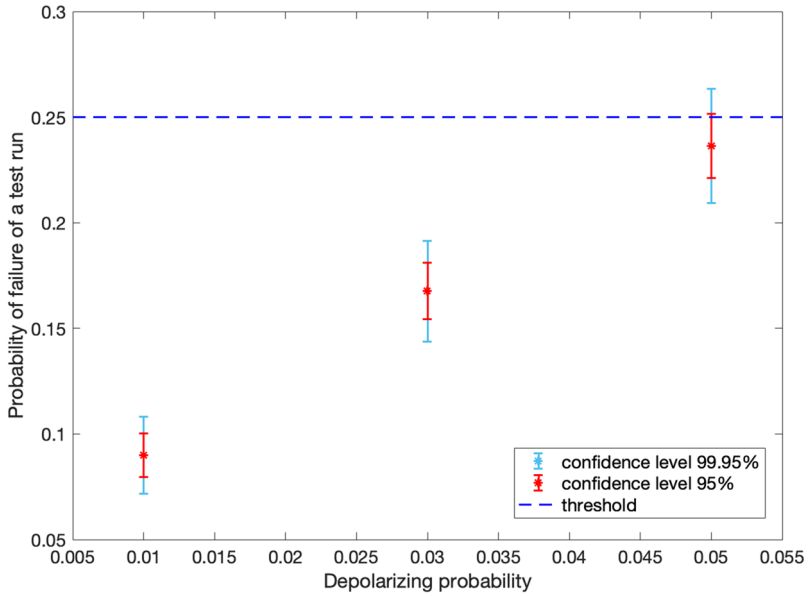

Figure 7. Probability of failure of a test run for different values of depolarizing probability in quantum gates. The blue dashed line represents the threshold 0.25 for w/t.

In order to obtain the optimum values for the protocol parameters w, t, and d, it is required to solve the optimization problem mentioned in[30], which is beyond the scope of this paper. Nevertheless, we provide an example by considering a depolarizing probability of 0.03 and $w = 1$. With these values, the only acceptable value for the number of test runs is $t = 5$. We run the protocol for 3000 times with 5 test runs and 6 computation runs. The resulting probability of correctness is 0.929 ± 0.0092, considering a confidence level of 95%. For more details on NetSquid simulation for this protocol please refer to Appendix D (Supplementary Information).

Benchmarking of quantum digital signature

QDS schemes can guarantee the unforgeability, nonrepudiation, and transferability of a signed message with information-theoretical security. Here, we consider the three-party QDS protocol proposed in[19]. The protocol is outlined Appendix C (Supplementary Information).

In the practical implementation of this protocol, various imperfections such as transmission loss and measurement error may adversely affect the performance of the protocol. In the following, the figures of merit for this protocol are discussed.

Figures of merit. We can define three main figures of merit for the security of this protocol. First of all, the probability of aborting under the assumption that all three parties are honest characterizes the robustness of the protocol. Another figure of merit is the probability of successful forging the signature by Bob. The third security criteria is the probability of repudiation, i.e., the probability that the signature sent by Alice is accepted by Bob, but when Bob forwards it to Charlie it is rejected. We denote the security bounds on these three probabilities by P_{abort}, P_{for}, and P_{rep}, respectively. The security level of the protocol is then defined as $\beta = \max\{P_{\text{abort}}, P_{\text{for}}, P_{\text{rep}}\}$.

Simulation results. In this subsection, the simulation results for the quantum digital signature protocol described in Appendix C (Supplementary Information) are presented. The number of transmitted qubits is assumed to be 5×10^4. We assume Alice and Bob are connected via an optical fibre with length L_{fib}. Similarly, the distance between Alice and Charlie is L_{fib}. The total loss of the system (excluding the loss of the optical fibre) is assumed to be 0.5. The attenuation coefficient of the optical fibre is 0.2 dB/km. We set the protocol parameters ε, ε_{PE}, a and r as $\varepsilon = 10^{-10}$, $\varepsilon_{PE} = 10^{-5}$, $a = 10^{-5}$, and $r = 0.1$. Here, ε_{PE} is the failure probability in calculating the upper bounds for error rates, r is the fraction of sifted key used in error estimation, and a and ε are small constants. For more information on these parameters please refer to Appendix C (Supplementary Information).

We consider different values for the length of optical fibre and evaluate the performance of the system in the presence of channel loss. Furthermore, two cases for the error in the measurement setup, denoted by e_d, are considered. The first case is the ideal case where there is no error, whereas in the second one $e_{\text{d}} = 0.015$.

According to Eq. (8) in Appendix C, we have $P_{\text{abort}} = 2\varepsilon_{PE} = 2 \times 10^{-5}$. As for P_{for}, our results show that $P_{\text{for}} = 10^{-4}$ for all cases. This is mainly because for our chosen parameter values, l is sufficiently large such that $\varepsilon_F \simeq \varepsilon/a = 10^{-5}$.

Table 4 shows the parameter P_{rep} for different values of L_{fib} and e_d. It can be seen that as fibre length increases, the security bound for probability of repudiation increases significantly. This mainly happens due to the reduction of the number of received signals, which results in a shorter signature. Hence, P_{rep} increases according to

Parameter values	P_{rep}
$L_{\text{fib}} = 5\,\text{km}, e_d = 0$	6.7×10^{-5}
$L_{\text{fib}} = 10\,\text{km}, e_d = 0$	0.008
$L_{\text{fib}} = 20, e_d = 0$	0.7
$L_{\text{fib}} = 5, e_d = 0.015$	0.1927
$L_{\text{fib}} = 10, e_d = 0.015$	0.698
$L_{\text{fib}} = 20, e_d = 0.015$	1

Table 4. P_{rep} for different values of L_{fib} and e_d.

Eq. (9) in Appendix C (Supplementary Information). Additionally, a shorter raw key leads to more statistical fluctuations in the estimation of error parameters [see Appendix C (Supplementary Information)], which results in a larger P_{rep}. For more details on NetSquid simulation for this protocol please refer to Appendix D (Supplementary Information).

Backward benchmarking

In the previous subsections, we presented a benchmarking method for quantum protocols based on determining fixed values for system parameters and evaluating the performance of the protocol considering various figures of merit. Another method to benchmark quantum protocols is to consider target values for figures of merit and optimize system parameters with the aim of minimizing hardware requirements while satisfying the target figures of merit. We refer to this method as "backward benchmarking". In[24], a method based on this type of benchmarking has been proposed to optimize entanglement generation and distribution in quantum networks using genetic algorithms. By appropriately redesigning the cost function used, this method can be adapted to evaluate the performance of various other quantum protocols and optimize hardware performance.

In this paper, as an example, we use the method proposed in[24] to benchmark the quantum money protocol. Specifically, our goal is to determine minimum requirements to guarantee the security of this protocol, i.e., $c > 0.875$, considering a fixed value for the storage time of qubits in the quantum memory. We are interested in answering the question of what are minimum viable improvements required for the quantum memory parameters T_1 and T_2, compared to their currently achievable values experimentally (referred to as "baseline values" in[24]), to achieve $c > 0.875$ for a desired fixed storage time.

To obtain the minimum requirements for a specific storage time, we consider an optimization problem with the following cost function

$$T_c = w_1 \Theta(c_{min} - c) + w_2 C(T_1', T_2'), \tag{16}$$

where the parameters w_1 and w_2 are the weights of the objectives in the cost function, $\Theta(\cdot)$ is the step function, and

$$C(T_1', T_2') = \frac{1}{\log_{T_{1b}'} T_1'} + \frac{1}{\log_{T_{2b}'} T_2'}. \tag{17}$$

In the above equation, the parameters T_i' and T_{ib}', for $i = 1, 2$, are in the range $[0, 1]$. Hence, T_i and T_{ib} are converted to a value in this range using the following equations:

$$\begin{aligned} T_i' &= \frac{T_i}{1 + T_i}, \\ T_{ib}' &= \frac{T_{ib}}{1 + T_{ib}}. \end{aligned} \tag{18}$$

By ensuring that both the base and the argument of the logarithm in (17) are in the range $[0, 1]$, we guarantee that the cost function reflects the progressive hardness of improving hardware parameters. By this we mean that to improve T_i slightly over T_{ib}, only a small cost is assigned. However, as T_i gets closer to its perfect value, the cost grows to infinity. This is meant to reflect the expectation that in an experimental setting, a hardware parameter becomes more difficult to improve as it approaches its perfect value. For further discussion on this point, see[24]. We employ a genetic algorithm-based optimization methodology to minimize the cost function in (16). For more information on the optimization procedure, please refer to[24].

As in section "Benchmarking of quantum money protocol", NetSquid is used to simulate the quantum money protocol. To obtain the parameter c, we use a block for 1000 qubit pairs and repeat the simulation for 5 times. For the baseline values, we choose $T_{1b} = 10\,\text{h}$ and $T_{2b} = 1s$. Other system parameters are the same as the ones chosen in section "Benchmarking of quantum money protocol". Table 5 shows the optimum solutions for values of T_1 and T_2. Comparing these values with the baseline values, it can be seen that T_2 requires much more improvement than T_1. This confirms that the main parameter limiting the performance of quantum money protocol is T_2. Another observation is that the optimal solution for T_2 is around three times the storage time of qubits in the quantum memory, which is in line with the results obtained in section "Benchmarking of quantum money protocol".

Storage time (s)	T_1 (h)	T_2 (s)
1	10.037	3.25
2	10.05	6.21
5	10.099	16.007

Table 5. Optimum solutions for values of T_1 and T_2.

Conclusion and future outlook

Quantum protocols enable distinctive functionalities such as secure communications and blind computation. To determine the requirements of quantum protocols and benchmark them against classical and post-quantum protocols, it is necessary to evaluate their performance considering different sources of system imperfection. Here, we considered several quantum protocols, namely quantum money, W-state based anonymous transmission, verifiable blind quantum computation, and quantum digital signature. We performed in-depth performance analysis for each protocol, mainly by use of NetSquid simulation platform.

First, we examined the effect of decoherence noise introduced by quantum memory in quantum money protocol. Our simulation results showed that the coherence time of quantum memory is the main parameter limiting the practical implementation of this protocol. To guarantee the security of this protocol, the coherence time of quantum memory is required to be at least three times the storage time of qubits. To enable longer than one second storage time while guaranteeing the security, it is necessary to improve hardware parameters, especially the coherence time of quantum memory.

Next, we considered W-state based anonymous transmission protocol and examined the degrading effect of different nonidealities such as decoherence noise of quantum memory, loss, and gate imperfections in the teleportation step. It can be inferred from the simulation results that the decoherence time constant of the quantum memory and the storage time of quantum particles play an important role in the fidelity of the teleported state. For instance, to achieve an average fidelity above 0.8 in this protocol, the storage time of the sender's and receiver's particles in the quantum memory must be less than half of the decoherence time constant of the quantum memory. This implies that aside from improving hardware parameters such as the decoherence time constant of quantum memory, minimizing the delay caused by the classical sub-protocols used in this protocol is of paramount importance. This can be achieved by using high-speed processors for the classical sub-protocols, and reducing the number of times the parity sub-protocol is repeated in the veto protocol, denoted by s. According to[27], the correctness of the veto protocol decreases with reducing s. This imposes a trade-off between the correctness of the anonymous transmission protocol and the fidelity of the teleported state. The simulation results presented in this work are a great tool for efficient choice of protocol and hardware parameters, especially the parameters of classical sub-protocols such as s.

We also evaluated the degrading effect of the transmission loss on the probability of protocol failure. Although W-state based anonymous transmission protocol is more robust to loss of particles compared to its GHZ-based counterpart, our numerical results show that the probability of failure significantly increases with loss. Further, it was shown that the probability of protocol failure increases significantly by increasing the number of protocol participants, N. For instance, with our chosen parameters, for a transmission loss of 1 dB the probability of protocol failure for $N = 4$ and $N = 8$ are about 0.82 and 0.96, respectively. This restricts the scalability of the protocol and implies that its implementation is feasible only with small number of participants and in short-range scenarios.

Another protocol considered in this paper was three-qubit VBQC. We examined the performance of a test run considering different noise levels at the quantum gates. Our simulation results showed that with our chosen parameters, for a depolarizing probability of 0.05 at quantum gates, it was not possible to guarantee the security and correctness of this protocol. Furthermore, it can be inferred from the simulation results that if the depolarizing probability at the gate with highest depolarizing noise is at most 0.03, it is feasible to implement this protocol, although for a limited range of protocol parameters, e.g., t and w. To extend the range of feasible protocol parameters, it is necessary to enhance the fidelity of the quantum gates reaching beyond 0.9775 (corresponding to a depolarizing probability 0f 0.03).

Finally, we investigated the performance of quantum digital signature protocol. We evaluated the effect of transmission loss and the error in the measurement setup on the security level of the protocol. Our simulation results showed that the transmission loss adversely affects the probability of repudiation significantly. To compensate for the degrading effect of loss, one can increase the number of transmitted qubits.

It is worth noting that in this paper, we have considered three-qubit VBQC protocol (we assumed three qubits at the server), which is a specific case of this protocol. One possible future research direction is to change the number of qubits at the server and examine the impact of this parameter. Moreover, other types of BQC such as multi-server BQC protocols[31–33] can be considered. Furthermore, in this work we have assumed equal depolarization probability for all quantum gates to provide benchmarks. It will be interesting to investigate the effect of each individual gate by considering different noise levels for quantum gates. Another possible future research direction is to investigate the robustness of the quantum money protocol to different sources of loss such as transmission loss and quantum memory loss. Finally, one can consider the generalized QDS protocol with more than three parties[34] and evaluate the scalability of this protocol in practical scenarios like metropolitan area networks.

In summary, in this paper we presented detailed performance analysis of several quantum protocols: quantum money, W-state based anonymous transmission, verifiable blind quantum computation, and quantum digital

signature. The simulation results presented in this paper provides a better understanding of advantages and limitations of these protocols and paves the way for efficient design and implementation of these protocols in future quantum networks.

Data availability

All data generated in this paper can be reproduced by the provided methodology. The code repository for all NetSquid simulations performed in this work is available at: https://github.com/LiaoChinTe/netsquid-simulation.

Received: 14 November 2021; Accepted: 24 February 2022
Published online: 28 March 2022

References

1. Acín, A. *et al.* The quantum technologies roadmap: A European community view. *N. J. Phys.* **20**, 080201 (2018).
2. Wehner, S., Elkouss, D. & Hanson, R. Quantum internet: A vision for the road ahead. *Science* **362**, eaam9288 (2018).
3. Pirandola, S. *et al.* Advances in quantum cryptography. *Adv. Opt. Photon.* **12**, 1012–1236 (2020).
4. Pirandola, S., Eisert, J., Weedbrook, C., Furusawa, A. & Braunstein, S. L. Advances in quantum teleportation. *Nat. Photon.* **9**, 641–652 (2015).
5. Wallucks, A., Marinković, I., Hensen, B., Stockill, R. & Gröblacher, S. A quantum memory at telecom wavelengths. *Nat. Phys.* **16**, 772–777 (2020).
6. Wang, Y. *et al.* Efficient quantum memory for single-photon polarization qubits. *Nat. Photon.* **13**, 346–351 (2019).
7. Korzh, B. *et al.* Demonstration of sub-3 ps temporal resolution with a superconducting nanowire single-photon detector. *Nat. Photon.* **14**, 250–255 (2020).
8. Caleffi, M., Chandra, D., Cuomo, D., Hassanpour, S. & Cacciapuoti, A. S. The rise of the quantum internet. *Computer* **53**, 67–72 (2020).
9. Cuomo, D., Caleffi, M. & Cacciapuoti, A. S. Towards a distributed quantum computing ecosystem. *IET Quantum Commun.* **1**, 3–8 (2020).
10. Sheng, Y.-B., Zhou, L. & Long, G.-L. One-step quantum secure direct communication. *Sci. Bull.* **67**, 367–374 (2021).
11. Chen, S.-S., Zhou, L., Zhong, W. & Sheng, Y.-B. Three-step three-party quantum secure direct communication. *Sci. China Phys. Mech. Astron.* **61**, 90312 (2018).
12. Long, G.-L. & Zhang, H. Drastic increase of channel capacity in quantum secure direct communication using masking. *Sci. Bull.* **66**, 1267–1269 (2021).
13. Qi, Z. *et al.* A 15-user quantum secure direct communication network. *Light Sci. Appl.* **10**, 183 (2021).
14. Zhou, L., Sheng, Y.-B. & Long, G.-L. Device-independent quantum secure direct communication against collective attacks. *Sci. Bull.* **65**, 12–20 (2020).
15. Sheng, Y.-B. & Zhou, L. Distributed secure quantum machine learning. *Sci. Bull.* **62**, 1025–1029 (2017).
16. Bozzio, M. *et al.* Experimental investigation of practical unforgeable quantum money. *npj Quantum Inf.* **4**, 5 (2018).
17. Amiri, R. & Arrazola, J. M. Quantum money with nearly optimal error tolerance. *Phys. Rev. A* **95**, 062334 (2017).
18. Kumar, N. Practically feasible robust quantum money with classical verification. *Cryptography* **3**, 26 (2019).
19. Amiri, R., Wallden, P., Kent, A. & Andersson, E. Secure quantum signatures using insecure quantum channels. *Phys. Rev. A* **93**, 032325 (2016).
20. Wallden, P., Dunjko, V., Kent, A. & Andersson, E. Quantum digital signatures with quantum-key-distribution components. *Phys. Rev. A* **91**, 042304 (2015).
21. Broadbent, A., Fitzsimons, J. & Kashefi, E. Universal blind quantum computation. In *2009 50th Annual IEEE Symposium on Foundations of Computer Science*, 517–526 (IEEE, 2009).
22. Fitzsimons, J. F. & Kashefi, E. Unconditionally verifiable blind quantum computation. *Phys. Rev. A* **96**, 012303 (2017).
23. Ben-Or, M., Crépeau, C., Gottesman, D., Hassidim, A. & Smith, A. Secure multiparty quantum computation with (only) a strict honest majority. In *2006 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS'06)*, 249–260 (IEEE, 2006).
24. da Silva, F. F., Torres-Knoop, A., Coopmans, T., Maier, D. & Wehner, S. Optimizing entanglement generation and distribution using genetic algorithms. *Quantum Sci. Technol.* **6**, 035007 (2021).
25. Coopmans, T. *et al.* Netsquid, a network simulator for quantum information using discrete events. *Commun. Phys.* **4**, 164 (2021).
26. Lipinska, V., Murta, G. & Wehner, S. Anonymous transmission in a noisy quantum network using the w state. *Phys. Rev. A* **98**, 052320 (2018).
27. 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).
28. Oh, S., Lee, S. & Lee, H.-W. Fidelity of quantum teleportation through noisy channels. *Phys. Rev. A* **66**, 022316 (2002).
29. Horodecki, M., Horodecki, P. & Horodecki, R. General teleportation channel, singlet fraction, and quasidistillation. *Phys. Rev. A* **60**, 1888 (1999).
30. Kashefi, E., Leichtle, D., Music, L. & Ollivier, H. Securing quantum computations in the NISQ era. *arXiv preprint*arXiv:2011.10005 *(2020).*
31. Morimae, T. & Fujii, K. Secure entanglement distillation for double-server blind quantum computation. *Phys. Rev. Lett.* **111**, 020502 (2013).
32. Li, Q., Chan, W. H., Wu, C. & Wen, Z. Triple-server blind quantum computation using entanglement swapping. *Phys. Rev. A* **89**, 040302 (2014).
33. Sano, Y. Multi-server blind quantum computation protocol with limited classical communication among servers. *arXiv preprint*arXiv:2106.05537 *(2021).*
34. Amiri, R., Abidin, A., Wallden, P. & Andersson, E. Unconditionally secure signatures. *IACR Cryptol. ePrint Arch.* **2016**, 739 (2016).

Acknowledgements

We acknowledge support of the European Union's Horizon 2020 Research and Innovation Program under grant agreement number 820445 (QIA). This work was supported by EPSRC grants EP/N003829/1.

Author contributions

C.L. performed NetSquid simulations. S.B. wrote the paper and contributed to parts of the coding. F.F.S. developed the optimization algorithm for backward benchmarking of quantum money protocol. E.K. advised on the execution of this study. All authors reviewed 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/s41598-022-08901-x.

Correspondence and requests for materials should be addressed to S.B.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.