IOP Publishing Quantum Sci. Technol. 4 (2019) 025009 https://doi.org/10.1088/2058-9565/ab03ac

Quantum Science and Technology

OPEN ACCESS

RECEIVED
4 October 2018

REVISED
28 January 2019

ACCEPTED FOR PUBLICATION
31 January 2019

PUBLISHED
20 February 2019

PAPER

Simple proof of confidentiality for private quantum channels in noisy environments

A Pirker[1,5,6], M Zwerger[1,2,5], V Dunjko[1,3], H J Briegel[1,4] and W Dür[1]

[1] Institut für Theoretische Physik, Universität Innsbruck, Technikerstraße 21a, A-6020 Innsbruck, Austria
[2] Departement Physik, Universität Basel, Klingelbergstraße 82, 4056 Basel, Switzerland
[3] Max-Planck-Institute of Quantum Optics, Hans-Kopfermann-Strasse 1, D-85748 Garching, Germany
[4] Fachbereich Philosophie, Universität Konstanz, Universitätsstraße 10, D-78464 Konstanz, Germany
[5] These authors contributed equally.
[6] Author to whom any correspondence should be addressed.

E-mail: alexander.pirker@student.uibk.ac.at

Keywords: quantum cryptography, quantum communication, measurement-based quantum computation

Abstract

Complete security proofs for quantum communication protocols can be notoriously involved, which convolutes their verification, and obfuscates the key physical insights the security finally relies on. In such cases, for the majority of the community, the utility of such proofs may be restricted. Here, we provide a simple proof of confidentiality for parallel quantum channels established via entanglement distillation based on hashing, in the presence of noise, and a malicious eavesdropper who is restricted only by the laws of quantum mechanics. The direct contribution lies in improving the linear confidentiality levels of recurrence-type entanglement distillation protocols to exponential levels for hashing protocols. The proof directly exploits the security relevant physical properties: measurement-based quantum computation with resource states and the separation of Bell-pairs from an eavesdropper. The proof also holds for situations where Eve has full control over the input states, and obtains all information about the operations and noise applied by the parties. The resulting state after hashing is private, i.e. disentangled from the eavesdropper. Moreover, the noise regimes for entanglement distillation and confidentiality do not coincide: confidentiality can be guaranteed even in situations where entanglement distillation fails. We extend our results to multiparty situations which are of special interest for secure quantum networks.

1. Introduction

Secure and private quantum communication is a concept of fundamental importance for emerging quantum technologies. The secure generation of a secret key for the encryption of classical data has received enormous attention in recent years [1–7], and is believed to be one of the key applications of quantum information science. Security has been shown under ever more general assumptions, finally arriving at device-independent proofs where the devices for secret key expansion are not trustworthy [8–10]. However, while establishing entanglement between two remote parties served as key ingredient in many security proofs of QKD, most existing proofs are not established by sharpening this intuition, i.e. they follow a more convoluted, tedious, and less straightforward route [2, 11–13].

Here we consider the problem of confidential or secure transmission of quantum information via quantum channels, equally important as QKD but far less studied. This task is closely related to the confidential generation of maximally entangled, distributed quantum states. Both are essential ingredients of quantum networks [14–16], quantum key agreement protocols [17–19], and distributed quantum computation [20]. In an idealized, noiseless situation a secure quantum channel, studied in [21–23], may be established in terms of teleporation [24] using a perfect Bell-pair. The situation turns out to be far less straightforward in a noisy scenario. Nevertheless, it was shown that private entanglement is feasible when considering noisy channels and perfect operations [25, 26], as well as noise in local operations for independent and identically distributed (i.i.d.)

[27] and non i.i.d. [28] situations. The latter works consider the recurrence-type entanglement distillation protocols (EDPs) [25, 26], which probabilistically increase the fidelity and factor out any eavesdropper with a linear rate of convergence in terms of initial states.

Hashing protocols [29–36] are one-way EDPs which overcome these limitations. They are deterministic and converge *exponentially fast* in terms of initial states towards several copies of a maximally entangled state. This enables for several confidential quantum channels in parallel, crucial for big quantum data transmission [37] and which is in contrast to recurrence-type EDPs.

In this paper we provide a proof of confidentiality for hashing protocols in a noisy setting where the eavesdropper has full control over all the initial states. Since the confidentiality of recurrence-type EDPs [25, 26] has been shown in similar scenarios [28], this alone is not too surprising, even though hashing enables for exponential confidentiality levels rather than linear ones. Nevertheless, due to the simplicity of the confidentiality proof we clearly identify the relevant elements of physical properties from which the formal claim follows: the purity of the target state for noiseless entanglement distillation protocols and the way one deals with noise in measurement-based quantum computation (MBQC) with resource states. We emphasize that both are not exploitable in a noisy gate-based implementation as we illustrate later. The interest of using such characteristics, arguably, goes beyond the direct cryptographic statement they are implying. What is more, we identify a regime of noise where privacy, or equivalently confidentiality, is feasible, whereas distillation is not. Furthermore we show that hashing establishes privacy even when the eavesdropper is provided with information regarding all noise processes occurring in Alice's and Bob's laboratory, which is one step towards device independence for protocols with a quantum output.

Early security proofs for QKD [7] rely on fault-tolerant quantum computation to reduce the problem of proving security to a noiseless setting, and utilize quantum random hashing [29] to verify the successful generation of entanglement. In contrast, our approach eliminates the necessity of fault-tolerant quantum computation by exploiting physical properties of MBQC with resource states, and we use hashing as an active tool to establish high-fidelity entangled pairs via entanglement distillation rather than verifying them. Other works [1, 4, 6] also use the existence of (one-way) EDPs. However, earlier works [1, 6, 7] lack a full treatment of the finite size setting, crucial for realistic regimes [11]. In contrast, here we analyze the finite size performance of hashing and explicitly provide confidentiality levels also in non-i.i.d. scenarios.

EDPs aim at distilling entanglement from a noisy ensemble of bi- or multipartite quantum states via local operations and measurements. Hashing protocols [29–36] form a specific subset of those protocols, which rely on the concept of likely subspaces [38], used in information theory, and universal hash functions [39], typically applied in the context of privacy amplification. Their operation is usually described on a large, noisy ensemble (called initial states) and one distills in the asymptotic limit a fraction of systems in a maximally entangled state, see appendix A for more details. However, it was shown that hashing via quantum gates fails in the presence of noise [40]. This drawback is overcome by measurement-based quantum information processing [41]. There, the desired quantum operation is realized via Bell-measurements between the input quantum state and the input qubits of a resource state, referred to as read-in measurements. Consequently the only source of noise within this computational approach is due to imperfect resource states and noisy Bell-measurements (which can be accounted for by an increased level of the noise acting on the resource state, see [40]). A measurement-based implementation of the hashing protocol, see appendix A.2, is capable of distilling entanglement for local depolarizing noise (LDN) up to 7% acting on each qubit of the resource state [40]. This is due to an observation made in [42]: LDN acting on the input qubits of the resource state can *virtually* be moved to the initial states. Furthermore, LDN noise acting on the output qubits of the resource state can be assumed to act afterwards, since it commutes with the read-in measurements. These observations provide insights how one deals with LDN in MBQC with resource states, a physical characteristic which is not directly usable in quantum circuits, see appendix A.2. More precisely, for gate-based implementations the situation is more complex and difficult to formalize in a useful way, since noise introduced by quantum gates gets highly correlated on propagating noise through the entire circuit.

In a multipartite setting, a measurement-based implementation of the hashing protocol might turn out to be very useful for large scale quantum network architectures which rely on e.g. GHZ states [43].

In this paper we will use the terms *confidential*, *secure*, *privacy*, *private states* and *private entanglement*. Therefore we want to clarify their relationship and their distinction before using them.

A communication channel, either classical or quantum, is referred to as confidential if an eavesdropper can not obtain any information regarding the data being transmitted. Nevertheless, the eavesdropper might change the data during transmission without being detected. Therefore we refer to privacy as the ability of two (or more) parties to establish a confidential communication channel. A communication channel is considered to be secure, if it is confidential and authenticated, where authenticated here means that the eavesdropper can not alter the data without being detected by the parties. In the quantum case we call a state private if it can be used to establish a confidential quantum channel, i.e. a state which is entangled between Alice and Bob but not entangled with the

eavesdropper. The term private state was already introduced in the context of QKD for generating classical keys from states with bound entanglement [44] and computing secret key capacities of quantum channels [45]. For that purpose [44, 45] consider additional systems, known as shield systems, to decouple an eavesdropper from maximally entangled states to generate a secure key between two parties. However, privacy or private states as we consider here, refer to the ability of establishing a confidential quantum channel without the notion of shield systems. The entanglement of such a state is then referred to as private entanglement.

For full formal definitions, proofs and supportive information we refer to the supplemental material. However, the confidentiality proof of hashing is self-contained in the main text.

2. Results

We consider two categories of players: protocol participants and Eve, the eavesdropper, from which the participants request their initial states $\rho^{(n)}$ used for entanglement distillation. The former, connected via classical authenticated channels, wish to distill m copies of a certain state $|\varphi\rangle$. In the bipartite setting, the state $|\varphi\rangle$ might correspond to a perfect Bell-pair [29] whereas in the mutlipartite setting to a specific multipartite state [30–36] . The latter distributes the initial states via noisy quantum channels and has full control over them. In particular, Eve might be fully entangled with all initial states, which corresponds to the most general scenario how initial states can be distributed.

Hashing in its original form assumes initial states of tensor product form, i.e. $\rho^{(n)} = \rho^{\otimes n}$ where ρ is a density operator of a multi-partite quantum state and n is asymptotically large. Furthermore, entanglement distillation will only be feasible if the entropy of the initial states is sufficiently low, see e.g. [29] for bipartite hashing.

To accommodate these requirements, we propose the following protocol: First the participants agree on a number of desired output systems m and a confidentiality level ε. From these values they compute the number of systems n which are necessary to meet both conditions, assuming the worst case entropy for the initial states. Then, the participants request $n + kn$ systems from Eve subject to entanglement distillation. They apply a local twirling operation which ensures that the systems are diagonal within the respective basis (for the bipartite protocol they twirl towards Werner form). Next, they sacrifice kn systems for parameter estimation in order to estimate the actual fidelity F relative to $|\varphi\rangle$ for each system. Depending on their estimate $\overline{F}$, they either abort the protocol because the fidelity is outside $[F_{\min}, F_{\max}]$ or they continue with a measurement-based implementation of the hashing protocol. Finally they output m systems. When generalizing to arbitrary initial states the protocol will be prepended by a symmetrization step.

To formalize our confidentiality criterion we recall some basic terminology introduced in [28]. We start with the definition of the noiseless ideal map $\mathcal{F}$, which takes as input the initial states and outputs, depending on parameter estimation, either the asymptotic state of the hashing protocol, $|\varphi\rangle\langle\varphi|^{\otimes m}$, or some output state, $\sigma^{\perp}_{\mathrm{PE}}$. For example, in a bipartite setting $|\varphi\rangle\langle\varphi|^{\otimes m} = |B_{00}\rangle\langle B_{00}|^{\otimes m}$ where $|B_{00}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. The ideal map $\mathcal{F}$ abstracts the entanglement distillation protocol for an initial state ρ as a process: internally it runs the real protocol for initial state ρ to its very end which succeeds with probability p_ρ, and depending on parameter estimation, it either replaces the final state with its asymptotic state, or it outputs whatever state was reached by the protocol, $\sigma^{\perp}_{\mathrm{PE}}$. This approach to define ideal functionality stems from well-established ideas in QKD [46]. Formally we define

$$(\mathcal{F} \otimes \mathrm{id}_E)(|\psi\rangle\langle\psi|_{\mathrm{PE}}) = p_\rho |\varphi\rangle\langle\varphi|^{\otimes m} \otimes \sigma_E \otimes |\mathrm{ok}\rangle\langle\mathrm{ok}|_f + (1 - p_\rho)\sigma^{\perp}_{\mathrm{PE}} \otimes |\mathrm{fail}\rangle\langle\mathrm{fail}|_f, \tag{1}$$

where $|\psi\rangle_{\mathrm{PE}}$ is a purification of the initial state ρ provided by Eve and p_ρ denotes the probability of the protocol succeeding for initial state ρ. The system f distinguishes the accepting from the aborting branch.

To analyze confidentiality taking into account realistic noisy scenarios, we define the noisy ideal map $\mathcal{F}^\alpha$, where α characterizes the level of noise, as $\mathcal{F}^\alpha = \mathcal{N}^\alpha \circ \mathcal{F}$, where $\mathcal{N}^\alpha$ denotes the noise process acting on the output qubits of the resource states of hashing.

We first clarify the noise processes we assume to act on the resource states of the measurement-based implementation of hashing, which motivate our definition of the ideal noisy map. We observe that there are a number of dominating sources of noise: noise on the resource states, noise on the read-in Bell measurements, and noise on the initial states subject to entanglement distillation.

For the noise acting on the resource states we assume i.i.d. LDN. This is physically reasonable due to the observations in [47], which shows that i.i.d. LDN provides an accurate approximation of noise acting on resource states if these states get generated locally via entanglement distillation.

The resource states for the measurement-based implementation of hashing consist only of input and output qubits, see appendix A.2 for further details. We denote the noise acting on the input qubits and output qubits of the resource states by $\mathcal{N}_{\mathrm{in}} = \prod_{j=1}^{n} \mathcal{D}_j(\alpha)$ and $\mathcal{N}_{\mathrm{out}} = \prod_{k=1}^{m} \mathcal{D}_k(\alpha)$ respectively where

$$\mathcal{D}_j(\alpha)\rho = \alpha\rho + \frac{1-\alpha}{4}(\rho + X_j\rho X_j + Y_j\rho Y_j + Z_j\rho Z_j), \tag{2}$$

with $\alpha \in [0,\ 1]$ quantifies the level of noise and the subscript j denotes the qubit on which the Pauli operators act on. Furthermore, we can take into account for the noise which the read-in Bell measurements introduce by a lower value of α in N_{in}, which we denote by β, see [40]. Hence, we have $\mathcal{N}_{\text{in}} = \prod_{j=1}^{n} \mathcal{D}_j(\beta)$.

Because we can now mathematically shift the noise from the input qubits of the resource states to the initial states, we decompose the ideal noisy map $\mathcal{F}^\alpha$ as the concatenation of noise acting on the initial states followed by the noiseless ideal hashing protocol and noise acting on the output qubits of the hashing protocol, i.e. $\mathcal{F}^\alpha = \mathcal{N}_{\text{out}} \circ \mathcal{F} \circ \mathcal{N}_{\text{in}}$. Because we can take into account for $\mathcal{N}_{\text{in}}$ in the parameter estimation step of the ideal map $\mathcal{F}$ we end up with $\mathcal{F}^\alpha = \mathcal{N}^\alpha \circ \mathcal{F}$, where we have defined $\mathcal{N}^\alpha = \mathcal{N}_{\text{out}}$.

This enables us now to precisely define the term confidentiality. In particular, we call the hashing protocol $\mathcal{E}^\alpha$ ε-confidential, if

$$\|\mathcal{E}^\alpha - \mathcal{F}^\alpha\|_\diamond \leqslant \varepsilon, \tag{3}$$

where $\|\Delta\|_\diamond = \sup_{k\in\mathbb{N}} \|\Delta \otimes \mathrm{id}_k\|_{\text{op},1}$ for a CPTP map Δ with $\|\Delta\|_{\text{op},1} \coloneqq \sup_{\|\rho\|_1 \leqslant 1} \|\Delta(\rho)\|_1$ and $\|\rho\|_1 = \mathrm{tr}\sqrt{\rho\rho^\dagger}$ denotes the 1-norm of a density operator ρ, see also [48].

Observe that the state $|\varphi\rangle\langle\varphi|^{\otimes m}$ in the accepting branch of $\mathcal{F}^\alpha$, see (1), is private, i.e. a state which is disentangled from Eve. This motivates the term privacy distillation.

We outline the remainder of this paper as follows: we start by estimating the rate of convergence of noiseless bipartite hashing for finitely many i.i.d. initial states. Next, we generalize this result to arbitrary initial states including the eavesdropper's system via the post-selection technique. This will finally imply the confidentiality guarantees for the noisy measurement-based implementation of hashing.

The hashing protocol [29] deterministically converges exponentially fast towards several copies of $|B_{00}\rangle$ for i.i.d. initial states. In particular, we find for the noiseless modified (i.e. our proposed) hashing protocol $\mathcal{E}$, taking $n + kn$ initial states ρ, that

$$\|\mathcal{E}(\rho^{\otimes n+kn}) - \mathcal{F}(\rho^{\otimes n+kn})\|_1 \leqslant 2[2\exp(-nx_1(\delta)) + 2^{-n\delta} + 2\exp(-(F_{\max} - F_{\min})^2\, kn/16)], \tag{4}$$

where $x_1(\delta) = 1/a_{\max}\left[(g_{\max}+\delta)\log\left(1 + \frac{\delta}{g_{\max}}\right) - \delta\right]$ and $a_{\max}$, $g_{\max}$ are constants depending on $F_{\min}$ and $F_{\max}$. The parameter δ stems from the hashing protocol [29] and affects the number of output systems $m = n(1 - S(\rho) - 2\delta)$ where $S(\rho)$ denotes the von Neumann entropy of ρ as well as the rate of convergence governed by (4). For our purposes we choose $\delta = n^{-1/5}$, see appendix C. In addition, the right-hand side of (4) approaches zero exponentially fast.

Equation (4) can be derived from the following observations, see also appendix C: the 1-norm induced distance of $\mathcal{E}(\rho^{\otimes n+kn})$ and $\mathcal{F}(\rho^{\otimes n+kn})$ is equal to the distance within the ok-branch, because $\mathcal{E}$ and $\mathcal{F}$ agree on the fail-branch. The protocol can fail due to three reasons where each type of failure occurs with a certain probability. The first one corresponds to the case that the ensemble of Bell pairs falls outside of the likely subspace and is given by $2\exp(-nx_1(n^{-1/5}))$. The second one bounds the probability of misidentifying the string by $\exp(-n^{4/5}\ln 2)$, and the third one bounds the failure probability of parameter estimation by $2\exp(-(F_{\max} - F_{\min})^2\, kn/16)$.

Nevertheless, (4) is insufficient to prove full cryptographic confidentiality, as it only concerns the systems of the participants and i.i.d. initial states. So the next step is to generalize (4) to arbitrary initial states including the system of Eve which is the topic of the next section.

In order to provide an estimate of (3) for bi- and multipartite hashing protocols in terms of i.i.d. initial states, e.g. (4), we proceed similar to the approach of [28]: first we relate the distance of the real and ideal map including Eve's purifying system at the beginning of the protocol to the distance between the respective maps concerning the systems of the participants only. Second we use the post-selection technique [46], which implies that the distance between the real and ideal map for any purification of the initial states is bounded by a specific pure state, a purification of the so called de-Finetti Hilbert–Schmidt state.

We eliminate the first issue by using an inherent characteristic of noiseless entanglement distillation protocols: the target state of such protocols shared between Alice and Bob is pure, provided the parameter estimation is passed. Therefore the state of Alice and Bob is independent of Eve, i.e. there is no residual entanglement to her. We formalize this intuition via the following observation, rigorously proven in appendix D: if the output of the real and ideal map, i.e. $\mathcal{E}$ and $\mathcal{F}$ respectively, differ at most ε for a particular initial state ρ, then they differ at most $4\sqrt{\varepsilon}$ on any purification $|\psi\rangle$ of ρ, i.e.

$$\|(\mathcal{E}\otimes\mathrm{id}_E - \mathcal{F}\otimes\mathrm{id}_E)(|\psi\rangle\langle\psi|_{ABE})\|_1 \leqslant 4\sqrt{\varepsilon}. \tag{5}$$

The next step is to relate non-i.i.d. initial states to i.i.d. initial states. Recall that the post-selection technique is applicable to permutation invariant maps only. Because hashing protocols are not permutation invariant maps,

we have to prepend the overall protocol by a symmetrization step in order to apply the post-selection technique. This finally enables us to prove confidentiality of hashing protocols according to (3) via the following theorem.

Theorem 1 (**Post-selection-based reduction technique**). *Let $\mathcal{E}^s$ be the real protocol and $\mathcal{F}^s$ the ideal protocol prepended by a symmetrization step (s) taking $n + kn$ initial states. Let $\mathcal{E}$ and $\mathcal{F}$ be the sub-protocols after symmetrization. Then we have*

$$\|\mathcal{E}^s - \mathcal{F}^s\|_\diamond \leqslant 4 g_{n+kn,d} \sqrt{\max_{\sigma_{AB}} \|(\mathcal{E} - \mathcal{F})(\sigma_{AB}^{\otimes n+kn})\|_1}\,, \tag{6}$$

where d denotes the dimension of an individual system and $g_{n+kn,d} = \binom{n + kn + d^2 - 1}{n} \leqslant (n + kn + 1)^{d^2-1}$.

The parameter d in theorem 1 corresponds to the dimension of each individual initial state, therefore it is constant for a specific protocol and we have for M participants that $d = 2^M$.

We sketch the proof of theorem 1 as follows: the post-selection technique of [46] implies that $\|\mathcal{E}^s - \mathcal{F}^s\|_\diamond = \sup_{|\psi\rangle_{ABE}} \|(\mathcal{E}^s - \mathcal{F}^s) \otimes id_E(|\psi\rangle\langle\psi|)\|_1$ is bound by evaluating this expression for a particular state, a purification of the de-Finetti Hilbert–Schmidt state. Hence we apply our previous observation, i.e. (5), to that particular initial state which reduces the confidentiality proof to i.i.d. initial states. For the complete proof of theorem 1 we refer to appendix E.

We now easily conclude confidentiality of the noiseless bipartite hashing protocol prepended by symmetrization by combining theorem 1 for $d = 4$ and (4) which leads to

$$\begin{aligned}\|\mathcal{E}^s - \mathcal{F}^s\|_\diamond \leqslant\ & 4\sqrt{2}\,(n + kn + 1)^{15} \\ & \times [2\exp(-n x_1(n^{-1/5})) + \exp(-n^{4/5}\ln 2) \\ & + 2\exp(-(F_{\max} - F_{\min})^2\, kn/16)]^{1/2}\,.\end{aligned} \tag{7}$$

Equation (7) analytically proves that arbitrary confidentiality levels can be achieved via the hashing protocol [29] and finally enables us to show confidentiality for a noisy measurement-based implementation of the hashing protocol.

Recall that the resource states, necessary for a measurement-based implementation of the hashing protocol, are subject to LDN acting on all qubits, $\mathcal{D}(\alpha) = \prod_{l=1}^{n} \mathcal{D}_l(\alpha)$ where $\mathcal{D}_l(\alpha)$ is defined in equation (2) and that we include the noise of a noisy Bell-measurement at the read-in in the value of α in (2), see [40]. For a more detailed discussion of this noise model we refer to [47] and appendix A.2.

The confidentiality proof for the noisy measurement-based implementation of hashing now concludes by using the following intuition from MBQC with resource states: the LDN on the input qubits can be moved, due to the symmetry of Bell-states, to the initial states whereas LDN acting on the output qubits can be assumed to act after the protocol. Therefore one is left with a noiseless hashing protocol generating pure states affected by LDN. We reiterate that such an approach is not directly applicable in the setting of gate-based implementations.

We sharpen this observation as follows: the resource states of the protocol consist only of input and output qubits, see appendix A.2 and , and according to [42] we can virtually move the noise acting on the input qubits to the initial states provided by Eve. Thus we deal with this part of the noise via a modification of parameter estimation, since the entropy of the initial states increases after virtually moving the noise. The noise acting on the output qubits of the resource states can be assumed to act after the protocol completes, as that noise commutes with the read-in Bell-measurements. This leaves us with a noiseless protocol followed by LDN acting on the output qubits, which just slightly depolarizes the pure Bell-pairs from noiseless hashing. Moreover, this noise stems from the apparatus so this does not jeopardize confidentiality. In particular, because LDN is a CPTP map, the contractivity of the 1-norm implies (see also appendix F) that

$$\|\mathcal{E}^{s,\alpha} - \mathcal{F}^{s,\alpha}\|_\diamond \leqslant \|\mathcal{E}^s - \mathcal{F}^s\|_\diamond\,, \tag{8}$$

where $\mathcal{E}^{s,\alpha}$ and $\mathcal{F}^{s,\alpha}$ denote the real and the ideal noisy hashing protocol prepended by symmetrization, and noise of strength $1 - \alpha$ of the form (2) acts on each qubit of the resource states independently and identically. Hence the noisy implementation offers the same confidentiality guarantees as the noiseless implementation, the protocol just simply aborts more often during parameter estimation.

We highlight that the proof of confidentiality for noisy hashing does not require any numeric evidence, whereas the proof in [28] for the distillation protocol [25] relies on numerical simulations. Furthermore the tolerable noise for post-selection is significantly higher, namely of the order of several percent per qubit compared to $O(10^{-20})$ in [28], although it should be mentioned that the noise models are different and cannot directly be compared.

Furthermore we find that there exists a regime of noise for bipartite hashing where privacy, or equivalently confidentiality, is achievable even though distillation is not feasible. For this regime, the privacy regime, hashing

decreases the fidelity of each output system relative to $|B_{00}\rangle$, i.e. the protocol washes out entanglement rather than distilling it, but nevertheless, any eavesdropper factors out. In contrast, if the noise level is within the distillation regime the fidelity of each output system relative to $|B_{00}\rangle$ increases, and, as a consequence, any eavesdropper factors out. For private states in the context of QKD a similar observation was made in [44], where it was shown that even though entanglement distillation is not feasible yet secure keys can still be generated from private states with bound entanglement.

It is interesting to qualitatively compare these findings to earlier works: in [27, 49] confidentiality aspects were studied in the framework of a gate-based implementation of the EDP of [25]. It was also found that the noise regimes for privacy and distillation do not coincide, but contrary to the results presented here, the privacy regime for the gate based implementation was found to be a subset of the distillation regime. For more details on those noise regimes we refer to appendix B.

We consider the scenario where the local apparatus leaks all the information about the noise processes realized (by the noisy resource states of the hashing protocol) to Eve as in [27, 28]. Theorem 7 of [28] states that if a real protocol $\mathcal{E}^{\alpha}$ is ε-confidential, then it is $2\sqrt{\varepsilon}$-confidential if the noise transcripts leak to Eve. The resulting states remain private and enable for confidential quantum channels.

The hashing protocol [29] can be generalized to multipartite quantum states [30–36], which is relevant for distributed quantum computation [20], quantum key agreement protocols [17–19] and quantum networks [14–16, 43]. Also for those protocols one shows their confidentiality by following the same line of argumentation, which can be found in appendix G.

3. Discussion

In summary we have analytically shown that noisy measurement-based implementations of bi- and multipartite hashing protocols establish exponential confidentiality levels. We directly exploited the properties of MBQC with resource states which leads, together with the purity of the asymptotic state of noiseless hashing and the post-selection technique, to a short, straightforward and transparent confidentiality proof.

Furthermore, the privacy and distillation regimes do not coincide, similarly to private states with bound entanglement in the context of QKD. In particular, there exists a regime of local i.i.d. noise where privacy is achievable, but distillation is not. In this regime, any eavesdropper is factored out despite no entanglement being distilled. Nevertheless, in both regimes the final states are disentangled from any eavesdropper, which enables for secure quantum channels, if the information regarding the noise processes do not leak to the eavesdropper. If this information leaks to the eavesdropper, confidential quantum channels are still feasible as the resulting states remain private.

Acknowledgments

This work was supported by the Austrian Science Fund (FWF): P28000-N27, P30937-N27 and SFB F40-FoQus F4012, by the Swiss National Science Foundation (SNSF) through Grant number PP00P2-150579, the Army Research Laboratory Center for Distributed Quantum Information via the project SciNet and the EU via the integrated project SIQS.

Appendix A. Bipartite hashing protocol and its measurement-based implementation

In this section of the supplementary material we provide a short review of the biparite hashing protocol [29], we introduce the measurement-based implementation thereof [40] and discuss its advantages over a gate-based approach.

In the following we denote the four Bell-basis states by $|B_{ij}\rangle = (id \otimes \sigma_x^j \sigma_z^i)|B_{00}\rangle$ where $i \in \{0, 1\}$ is referred to as the phase bit, $j \in \{0, 1\}$ is referred to as the amplitude bit of $|B_{ij}\rangle$ and $|B_{00}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$.

A.1. Entanglement distillation via hashing

EDPs distill a maximally entangled state from several noisy copies provided the initial fidelity, defined as $F(\rho, \sigma) = \mathrm{tr}\sqrt{\rho^{1/2}\sigma\rho^{1/2}}$ for density operators ρ and σ where $\sigma = |\varphi\rangle\langle\varphi|$ (the desired target state), is sufficiently high. Several protocols have been proposed for this task, which we divide into two categories depending on the number of systems they utilize within each basic distillation step. In the first group we have recurrence-type protocols [25, 26] which work pair-wise, whereas in the second group we have so-called hashing-type protocols [29] that operate, in principle, on the entire ensemble. Common to both classes of protocols is that they utilize local operations, measurements and classical communication.

Recurrence-type protocols are robust against local noise in both the gate-based [50] and measurement-based implementations [42]. In contrast, the gate-based implementations of hashing-type protocols are fragile with respect to noise of the local apparatus as we will discuss briefly.

The hashing protocol [29] is an EDP which operates on a large ensemble of noisy initial states in an iterative manner. In its standard version, the participants assume to receive n copies of an initial state ρ, where ρ is a two qubit density operator diagonal in the Bell-basis. The hashing protocol outputs $m = n(1 - S(\rho))$ systems in the asymptotic limit where $S(\rho) < 1$ denotes the von-Neumann entropy of ρ. At each basic distillation step, which we also refer to as a round, the participants apply local operations according to a string drawn uniformly at random and followed by a controlled NOT into one target state. More precisely, they accumulate the phase and/or amplitude bit i and j of $\rho = \sum_{i,j} p_{ij} |B_{ij}\rangle \langle B_{ij}|$ of each individual pair into one target system via several controlled NOTs. Recall that such a bilateral controlled NOT transforms a tensor product of two Bell-states $|B_{i_1 j_1}\rangle$ and $|B_{i_2 j_2}\rangle$ to the tensor-product state $|B_{i_1 \oplus i_2 j_1}\rangle |B_{i_1 j_1 \oplus j_2}\rangle$. Next, the parties measure the target Bell-pair which is determined by the string. This measurement reveals essentially one bit of parity information about the remaining ensemble, thereby purifying it (as the mixedness of a state can be interpreted as a lack of classical information). The basic distillation step is iterated several times and in the end a fraction of purified systems remains.

Hashing protocols rely on two fundamental concepts related to classical coding theory: likely subspace encoding and universal hashing. The idea of likely subspace encoding for ensembles of quantum states was first mentioned, to our knowledge, in [38]. There it was proven that an asymptotic ensemble of i.i.d. quantum states $\rho^{\otimes n}$ where $\rho = \sum_i p_i |v_i\rangle \langle v_i|$ is a density operator which receives almost all its weight from a small subspace spanned by so-called likely sequences $\{\bigotimes_k |v_{i_k^{(j)}}\rangle \langle v_{i_k^{(j)}}|\}_{j \in J}$ where one identifies a specific sequence $\bigotimes_k |v_{i_k}\rangle \langle v_{i_k}|$ with the bit string $(i_1, \ldots, i_n)$. More precisely, the probability of finding a particular sequence $(j_1, \ldots, j_n)$ that is outside this likely subspace can be made arbitrarily small in terms of the number of copies n of ρ. In case of the hashing protocol the vectors $|v_i\rangle$ in $\rho = \sum_i p_i |v_i\rangle \langle v_i|$ of the initial states $\rho^{\otimes n}$ correspond to individual Bell-states $|B_{ij}\rangle$. The original proposal of the likely subspace in [38] relies on the weak law of large numbers, which is an asymptotic statement. Universal hashing [39] is a widely studied concept which turned out especially useful in privacy amplification [51], a critical part in quantum key distribution protocols. Privacy amplification minimizes the amount of information an eavesdropper has with respect to a generated key. For that purpose the participants use so-called *universal*$_2$ function families. A family of functions $\mathcal{G} = \{g_i : A \to B\}_{i \in I}$ is said to be *universal*$_2$ if for any $x \neq y \in A$ the probability that $g_i(x) = g_i(y)$ is at most $1/|B|$ when g_i is chosen uniformly at random from $\mathcal{G}$.

One basic distillation step of the hashing protocol comprises the following steps: one participant draws a string $s \in \{0, 1, 2, 3\}^n$ (which we also refer to as parity hash string) uniformly at random, corresponding to a universal hash function. Next, the participant classically communicates s to the other participant and both perform, according to s, local operations and bilateral controlled NOTs on their parts of the quantum states. Depending on $s_t \in \{0, 1, 2, 3\}$ they bypass ($s_t = 0$) or they accumulate either the amplitude bit j ($s_t = 1$), the phase bit i ($s_t = 2$) or both, amplitude and phase bit $i \oplus j$, ($s_t = 3$) for the Bell-pair $|B_{ij}\rangle$ indexed by $1 \leqslant t \leqslant n$ into the first pair for which $s_t \neq 0$ via a bilateral controlled NOT. Finally, they measure both parts of this target system using the Z observable which reveals almost one bit of parity information about the remaining ensemble. This basic distillation step is iterated $n - m$ times, thereby collecting sufficient amount of information regarding parities about the remaining quantum systems. The parity information is finally used to restore the systems to the $|B_{00}\rangle^{\otimes m}$ state. For further detsails on the hashing protocol, we refer the reader to [29].

If one considers instead of asymptotic ensembles an initial ensemble of finite size n, bipartite hashing can still be used to distill entanglement. For finitely many initial states slightly fewer systems with a finite infidelity (i.e. there is a non-zero deviation relative to the state $|B_{00}\rangle^{\otimes m}$) will be distilled. More precisely, for finite size hashing the number of output systems is $m = n(1 - S(\rho) - 2\delta)$ where the tunable parameter δ characterizes the width of the likely subspace. The parameter δ turns out to be crucial when determining the rate of convergence towards $|B_{00}\rangle^{\otimes m}$ and we will choose for our purposes $\delta = n^{-1/5}$ later.

There also exist extensions of the bipartite hashing protocol to a multipartite setting allowing the distillation of two colorable graph states [30], all graph states [31], GHZ states [32, 33], CSS states [34] and stabilizer states [35, 36]. Conceptually those types of protocols rely on the same ideas as bipartite hashing. Again, local parity collecting operations are used to reveal information about the remaining ensemble. They are especially well-suited to distill resource states for measurement-based implementations of particular quantum tasks such as quantum error correction.

In the main text we have outlined the proof of confidentiality of the hashing protocol for two colorable graph states [30] and we provide a detailed description and a complete proof of confidentiality thereof within this supplementary material.

A.2. Measurement-based implementation

One alternative to the gate-based implementation of a quantum circuit is MBQC [52, 53]. A quantum operation $\mathcal{O}$ can be implemented by coupling the input qubits via Bell measurements to a universal resource state, e.g. a 2D cluster state [54]. For circuits which contain only gates from the Clifford group and Pauli measurements one can also use an optimized, special purpose resource state of minimal size [41]. This resource state will consist of only $n + m$ qubits for a circuit which maps n qubits to m qubits. Hashing protocols, like most other EDPs, belong to this class of circuits and thus allow for such a minimal size measurement-based implementation. The results of the Bell measurements at the read-in determine both the results of the parity measurements of the hashing protocol as well as the Pauli byproduct operators on the final output states. For more informations and examples see [28, 55].

The noiseless implementation of the hashing protocol produces asymptotically perfect Bell-pairs. Therefore any eavesdropper is factored out, in the limit, guaranteeing perfect confidentiality. But even if i.i.d. LDN acts on the quantum gates, any gate-based approach fails [40]. This is due to the $O(n)$ bilateral CNOTs within every distillation round, which washes out all information from the initial states. Hence the gate-based implementation of hashing is limited to the noiseless scenario only.

This drawback is overcome by a measurement-based approach [40]. A measurement-based implementation of the hashing protocol is rather straightforward: a sequence of parity hash strings is drawn uniformly at random by one participant and classically communicated to all other participants. They construct the corresponding resource states according to that particular sequence. These resource states are finally coupled to the initial states via Bell-measurements which implements the hashing protocol in a measurement-based fashion.

Since all gates of the hashing protocol are elements of the Clifford group the resource states consist only of input and output qubits, see discussion above. This implies that the resource states are of minimal size and therefore optimal with respect to the number of qubits which need to be stored temporarily.

In [40] it was shown that a measurement-based implementation of the hashing protocol [29] is capable of distilling entanglement for imperfect resource states and imperfect read-in Bell-measurements. There the resource states are affected by i.i.d. local LDN of the form $\mathcal{D}(\alpha) = \prod_{l=1}^{n} \mathcal{D}_l(\alpha)$ acting on all qubits of the resource states where

$$\mathcal{D}_j(\alpha)\rho = \alpha\rho + \frac{1-\alpha}{4}(\rho + X_j\rho X_j + Y_j\rho Y_j + Z_j\rho Z_j) \tag{A1}$$

and α characterizes the strength of the noise. In particular, the measurement-based implementation of hashing tolerates up to 7% of noise acting on each qubit of the resource states [40]. In [56], it was shown that any local noise process can be brought into a local depolarizing form. This observation also motivated the noise model of LDN chosen in [42] to study measurement-based recurrence-type distillation protocols. There it was shown that the measurement-based implementation of recurrence-type distillation protocols is capable of tolerating up to 24% of noise acting on each qubit of the resource states. Furthermore, as studied in [47], local i.i.d. depolarizing noise provides an accurate and reasonable approximation if one generates the resource states via entanglement distillation. The generation of resource states via entanglement distillation also provides an efficient scheme to create high-fidelity resource states, crucial for accurate MBQC via resource states.

The reason why a measurement-based implementation of the hashing protocol in the presence of i.i.d. LDN of the form $\mathcal{D}(\alpha)$ works is due to a fundamental observation made in [42]: if the resource states undergo a LDN of the form $\mathcal{D}(\alpha) = \prod_{l=1}^{n} \mathcal{D}_l(\alpha)$ then one can *virtually* exchange the location of the LDN when followed by a Bell-measurement, i.e. $\mathcal{P}\mathcal{D}_1(\alpha)\rho = \mathcal{P}\mathcal{D}_2(\alpha)\rho$ where $\mathcal{P}\rho = P_B\rho P_B^\dagger$ and P_B denotes a projector on a Bell-state. Intuitively speaking, as $P_B = |B_{ij}\rangle\langle B_{ij}|$, this is due the symmetry $(\mathrm{id}\otimes\sigma)|B_{ij}\rangle = (\sigma\otimes\mathrm{id})|B_{ij}\rangle$ up to a global phase where σ is a Pauli operator. This enables us to effectively move the noise acting on the input qubits of the resource states to the input state (as we couple the input state to the resource states via Bell-measurements). We emphasize that this holds for LDN of the form $\mathcal{D}(\alpha) = \prod_{l=1}^{n} \mathcal{D}_l(\alpha)$ and, more importantly, this can not be done within the circuit model even though the gate-based and measurement-based approach to quantum computation are computationally equivalent. In particular, computational equivalence does not necessarily imply equivalent robustness with respect to noise. This observation becomes more clear when one considers the noise processes as being part of the protocol. In the measurement-based scenario with resource states, the observation of [42] implies that the i.i.d. LDN acting on the input qubits of the resource states can effectively be moved to the initial states, see discussion above. The i.i.d. LDN acting on the output qubits can be applied afterwards, because the quantum computation at hand is performed in terms of Bell-measurements at the read-in. This leaves one with a perfect quantum operation on a modifed input state, where i.i.d. LDN is applied, followed by the noise process of the output qubits. In [57] this observation was applied to measurement-based quantum communication, where it was shown that very high error thresholds (of the order of 10 % per qubit) can be obtained. In contrast, in the gate-based approach noise accumulates through repeatedly applying quantum gates. Furthermore, on commuting noise through the gates of a quantum circuit towards the input, the

noise processes might get correlated due to commutation relations, maybe ending up in correlated noise rather than i.i.d. LDN acting on the input state. So to summarize, this observation shows that at least for i.i.d. LDN the measurement- and gate-based approach are not equivalent.

To summarize, the measurement-based approach permits a noisy implementation of the hashing protocol whereas a standard gate-based implementation fails in the presence of noise.

Appendix B. Noise regimes

In the main text we identified two different regimes of i.i.d. LDN of the form $\mathcal{D}(\alpha) = \prod_{l=1}^{n} \mathcal{D}_l(\alpha)$, where $\mathcal{D}_l(\alpha)$ is defined via (A1), acting on the resource states of the measurement-based implementation of hashing: privacy and distillation regime. Within the first regime any eavesdropper factors out but no entanglement will be distilled. In particular, for bipartite hashing, the fidelity relative to $|B_{00}\rangle$ will decrease due to the protocol. In contrast, in the distillation regime any eavesdropper is factored out and entanglement is distilled, i.e. the fidelity relative to the target state increases.

To see this we recall the conditions on the noise parameters for distillation and privacy. The noiseless hashing protocol distills perfect Bell pairs in the asymptotic limit of infinitely many initial states in Werner form as soon as their fidelity exceeds $F_{\text{crit}} = 0.8107$, see [29]. In this case the final Bell pairs are private (and thus confidentiality is guaranteed) and F_{crit} can be translated to $q_{\text{crit}} = (4F_{\text{crit}} - 1)/3 \approx 0.7476$. In the noisy case one has two conditions for the noise parameters α and q, which quantify the level of noise on the resource states and the fidelity of the initial states, respectively (see also [42]) for asymptotic ensemble sizes:

$$\alpha^2 q > q_{\text{crit}} \tag{B1}$$

and

$$\alpha^2 > q. \tag{B2}$$

Here, (B1) guarantees that the fidelity of the initial states, after the noise from the resource states is mapped to the initial states, see the previous section and [42], exceeds the threshold value q_{crit}. In this case the output pairs will be private. The second condition, (B2), ensures that the fidelity of the output pairs is larger than the fidelity of the input pairs. From this one sees that for privacy one only needs to fulfill (B1), whereas both (B1) and (B2) need to hold for distillation. Observe that (B1) is a condition due to the noise acting on the input qubits (thereby increasing the required fidelity of the initial states to succeed hashing) whereas condition (B2) stems from the noise applied to the output qubits (which depolarizes the perfect Bell-pairs produced by noiseless hashing in the asymptotic limit). This means that the parameters α and q are more constrained if one aims for increasing entanglement, as compared to the case of privacy. We summarize these findings in figure B1.

This observation provides a clear distinction between privacy and distillation regime for asymptotic ensembles: both regimes, distillation and privacy, have in common that any eavesdropper factors out due to the protocol but they differ with respect to whether entanglement is distilled or not. This motivates the term

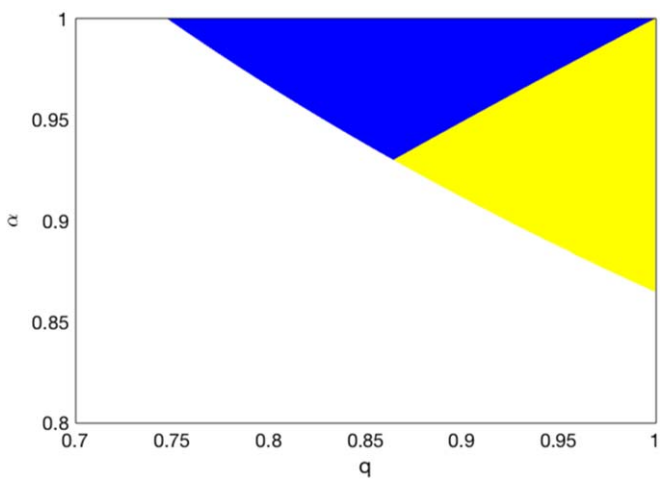

Figure B1. Visualization of the different regimes in the α–q plane (only the upper right corner of the entire plane is shown). In the white area neither privacy nor distillation is achieved. In the entire colored area privacy is guaranteed, but only in the blue area one has distillation. This means that there is a parameter regime (yellow area), where one has privacy despite the fact that the fidelity of the Bell pairs does not increase during the distillation.

quantum privacy distillation for the proposed overall protocol as there are noise regimes where the protocol offers privacy, or equivalently private entanglement, without achieving distillation.

A similar situation arises in the finite size case. Here, the modifications will be that q_{crit} in (B1) is no longer directly related to F_{crit} and that (B2) needs to be modified to

$$\alpha^2 q_{\text{out}}(n, F) > q_{\text{in}}. \tag{B3}$$

Here, $q_{\text{out}}(n, F)$ quantifies the level of noise on the output pairs of the hashing protocol for n initial states with fidelity F. It can be obtained from the bound on the fidelity of the output pairs. There will again be two different regimes, and the distillation regime will be smaller than the privacy regime due to the fact that it is more constrained (there are two inequalities to be satisfied, whereas there is only one for confidentiality).

Appendix C. Rate of convergence of noiseless bipartite hashing for i.i.d. initial states

Here we provide the proof of equation (4) of the main text for $\delta = n^{-1/5}$ summarized within the following Theorem.

Theorem 2 (**Convergence for i.i.d. initial states**). *Let $\mathcal{E}$ be the real protocol and $\mathcal{F}$ the ideal protocol taking $n + kn$ initial states. Furthermore, let $x_1(\delta) = 1/a_{\max}\left[(g_{\max}+\delta)\log\left(1+\frac{\delta}{g_{\max}}\right) - \delta\right]$ where $a_{\max}$ and $g_{\max}$ are constants depending on $F_{\min}$ and $F_{\max}$. Then we have for all initial states ρ that*

$$\|\mathcal{E}(\rho^{\otimes n+kn}) - \mathcal{F}(\rho^{\otimes n+kn})\|_1 \leqslant 2[2\exp(-nx_1(n^{-1/5})) + \exp(-n^{4/5}\ln 2) + 2\exp(-(F_{\max} - F_{\min})^2 kn/16)]. \tag{C1}$$

Furthermore, the right-hand side of equation (4) of the main text approaches exponentially fast zero.

Proof. Because the ideal and the real map are identical in the aborting branch, we find for the initial states $\rho^{\otimes n+kn}$ that

$$\|\mathcal{E}(\rho^{\otimes n+kn}) - \mathcal{F}(\rho^{\otimes n+kn})\|_1 = p_\rho \|\sigma_{AB} - |B_{00}\rangle\langle B_{00}|^{\otimes m}\| \leqslant \varepsilon_{\text{H}} \tag{C2}$$

where σ_{AB} denotes the state of the hashing protocol after $n - m$ rounds and p_ρ the success probability for initial state ρ. Thus we need to estimate ε_{H}. Because we twirl the initial states towards Werner form we assume from now on that they are of Werner form.

The hashing protocol can fail due to two reasons, see [29]: the string corresponding to the initial states falls outside the likely subspace or, after $n - m$ rounds two or even more configurations are compatible with the total parity information, i.e. they can not be distinguished from each other.

By denoting this failure probabilities by p_1' and p_2' and the corresponding states after the protocol by σ_1 and σ_2 respectively, we find that the total failure probability p_f' of the hashing protocol satisfies $p_f' = p_1' + p_2'$. We also observe that if the parameter estimation was accurate the state after the protocol completes, i.e. σ_{AB} of (C2), is given by

$$\sigma_{AB} = (1 - p_f')|B_{00}\rangle\langle B_{00}|^{\otimes m} + \sum_{i=1}^{2} p_i' \sigma_i. \tag{C3}$$

More precisely, with probability $1 - p_f'$ we are able to restore the output of the hashing protocol to m copies of $|B_{00}\rangle$ and we end up with probabilities p_1' and p_2' in the state σ_1 and σ_2 respectively. This implies for (C2) that

$$\|\sigma_{AB} - |B_{00}\rangle\langle B_{00}|^{\otimes m}\|_1 \leqslant 2(p_1' + p_2') \tag{C4}$$

via the triangle inequality for the case whenever parameter estimation is accurate.

Additionally the overall protocol can fail due to the following observation: the parameter estimation provides an estimate $\overline{F}$ for the fidelity F which is accepted by the participants, but F is actually outside the agreed range $[F_{\min}, F_{\max}]$. In that case Alice and Bob run hashing even though the protocol will either fail (since the initial fidelity is too low) or the fidelity is too high to provide accurate confidentiality estimates[7]. This observation in turn implies that the state after hashing within the ok-branch is maximum far from the asymptotic state of the hashing protocol, i.e.

$$\|\sigma_{AB} - |B_{00}\rangle\langle B_{00}|^{\otimes m}\|_1 \leqslant 2. \tag{C5}$$

[7] The hashing protocol requires $F > F_{\text{crit}}$ where $F_{\text{crit}} = 0.8107$ to distill entanglement from the initial states. The restriction that $F < F_{\max}$ is due to the applicability of Bennett's inequality which requires bounded random variables. However, for the noisy implementation of the hashing protocol this criterion will be met automatically as the resource states for the measurement-based implementation undergo an i.i.d. LDN process.

Nevertheless, the probability of the protocol succeeding for initial state ρ also takes into account for parameter estimation succeeding, i.e. $p_\rho = p_3' \cdot p'$ where p_3' denotes the probability of parameter estimation succeeding for initial state ρ. Therefore, if Alice and Bob mistakenly run hashing even if they should have aborted we find via (C5) for (C2) that

$$p_\rho \|\sigma_{AB} - |B_{00}\rangle\langle B_{00}|^{\otimes m}\|_1 \leqslant 2p_3'. \tag{C6}$$

So to summarize we obtain for an arbitrary initial state ρ by combining (C4) and (C6) that

$$p_\rho \|\sigma_{AB} - |B_{00}\rangle\langle B_{00}|^{\otimes m}\|_1 \leqslant 2(p_1' + p_2' + p_3'). \tag{C7}$$

Thus we are left to provide upper bounds for (the unknown) probabilities p_1', p_2' and p_3' respectively, i.e. we need to find p_1, p_2 and p_3 such that $p_i' \leqslant p_i$ for $1 \leqslant i \leqslant 3$ because this implies for (C7) that

$$p_\rho \|\sigma_{AB} - |B_{00}\rangle\langle B_{00}|^{\otimes m}\|_1 \leqslant 2(p_1 + p_2 + p_3). \tag{C8}$$

We derive a bound for the probability of falling outside the likely subspace p_1 via the Bennett inequality [58]. Bennett's inequality [58] states that we have for X_1 ,.., X_n independent random variables, where $|X_i| \leqslant a$ almost-surely and the expected value of X_i is zero w.l.o.g., that

$$\Pr\left(\left|\sum_{i=1}^{n} X_i\right| > t\right) \leqslant 2\exp\left(-\frac{n\sigma^2}{a^2}h\left(\frac{at}{n\sigma^2}\right)\right) \tag{C9}$$

where $\sigma^2 = 1/n\sum_{i=1}^{n}\mathrm{Var}X_i$ and $h(u) = (1+u)\log(1+u) - u$ [8].

For the hashing protocol the random variables X_i take the values $X_i(k, l) := -\log_2 p_{kl} - S(\rho)$ where $\rho = \sum_{k,l=0}^{1} p_{kl}|B_{kl}\rangle\langle B_{kl}|$ and $S(\rho) = -\sum_{k,l=0}^{1} p_{kl}\log_2 p_{kl}$ denotes the von-Neumann entropy. The von-Neumann entropy simplifies for states in Werner form to $S(\rho) = -F\log_2(F) - (1-F)\log_2((1-F)/3) =: S(F)$.

The i.i.d. assumption implies that all X_i are independent and identical distributed (therefore we will subsequently denote them by the random variable X), thus we find $\sigma^2 = 1/n\sum_{i=1}^{n}\mathrm{Var}X_i = \mathrm{Var}X =: V(F)$. Hence we have

$$\begin{aligned} V(F) = \mathrm{Var}X &= \sum_{k,l} p_{kl}(-\log_2 p_{kl} - S(F))^2 \\ &= \sum_{k,l} p_{kl}(\log_2^2 p_{kl} + 2S(F)\log_2 p_{kl} + S^2(F)) \\ &= \sum_{k,l} p_{kl}\log_2^2 p_{kl} + 2S(F)p_{kl}\log_2 p_{kl} + p_{kl}S^2(F) \\ &= \sum_{k,l} p_{kl}\log_2^2 p_{kl} + 2S(F)(-S(F)) + S^2(F) \\ &= F\log_2^2 F + (1-F)\log_2^2((1-F)/3) - S^2(F). \end{aligned} \tag{C10}$$

We observe that the random variable X is bounded. More precisely, we have $|X(k, l)| = |\log_2 p_{kl} + S(F)| \leqslant |\log_2((1-F)/3)| + S(F) =: a(F)$ because $|\log_2((1-F)/3)| > |\log_2 F|$ for $F > 0.8107$ (which is the minimum required fidelity for Werner states by the hashing protocol).

The next step is to insert $t = n\delta$, $a = a(F)$ and $\sigma^2 = V(F)$ in (C9) which yields by denoting the left-hand-side of (C9) by p_1

$$\begin{aligned} p_1 &\leqslant 2\exp\left(\frac{-nV(F)}{a^2(F)}h\left(\frac{a(F)n\delta}{nV(F)}\right)\right) \\ &= 2\exp\left\{\frac{-nV(F)}{a^2(F)}\left[\left(1+\frac{a(F)\delta}{V(F)}\right)\log\left(1+\frac{a(F)\delta}{V(F)}\right) - \frac{a(F)\delta}{V(F)}\right]\right\} \\ &= 2\exp\left\{\frac{-n}{a(F)}\left[\left(\frac{V(F)}{a(F)}+\delta\right)\log\left(1+\frac{a(F)\delta}{V(F)}\right) - \delta\right]\right\}. \end{aligned} \tag{C11}$$

By defining $g(F) = \frac{V(F)}{a(F)}$ we rewrite the previous inequality as

$$p_1 \leqslant 2\exp\left\{\frac{-n}{a(F)}\left[(g(F)+\delta)\log\left(1+\frac{\delta}{g(F)}\right) - \delta\right]\right\}. \tag{C12}$$

[8] Observe that Bennett's inequality is only applicable to bounded random variables, which is also the reason why we propose to accept only initial states where the fidelity is within an agreed range $[F_{\min}, F_{\max}]$.

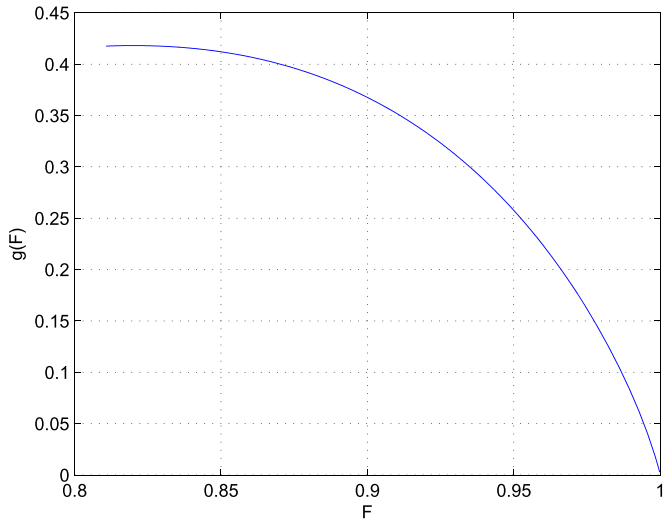

Figure C1. Plot of the function $g(F)$. Observe that g is strictly monotonic decreasing for $F \in [0.82,\ 1)$.

We observe that (C12) depends on the fidelity F of the initial states which is inappropriate for confidentiality estimates. In order to obtain a bound which is independent of the fidelity of the initial states we use that Alice and Bob only run the hashing protocol if $F \in [F_{\min},\ F_{\max}]$. We observe that (C12) is maximized whenever $\frac{n}{a(F)}[(g(F)+\delta)\log\left(1+\frac{\delta}{g(F)}\right)-\delta]$ is minimal because $(g(F)+\delta)\log\left(1+\frac{\delta}{g(F)}\right)-\delta \geqslant 0$ which follows from $\log(1+x) \geqslant \frac{x}{x+1}$, $n > 0$ and $a(F) > 0$.

For that purpose we show that the function $y(x) = (x+b)\log(1+b/x) - b = (x+b)(\log(x+b) - \log(x)) - b$ is strictly monotonic decreasing in x. We obtain for the first derivative of y that

$$\begin{aligned} y'(x) &= \log(x+b) + \frac{x+b}{x+b} - \left(\log(x) + \frac{x+b}{x}\right) \\ &= \log(x+b) + 1 - \log(x) - 1 - \frac{b}{x} \\ &= \log\left(\frac{x+b}{x}\right) - \frac{b}{x} = \log\left(1+\frac{b}{x}\right) - \frac{b}{x} \leqslant 0 \end{aligned} \tag{C13}$$

since $\log(1+z) \leqslant z$. Thus $(g(F)+\delta)\log\left(1+\frac{\delta}{g(F)}\right)-\delta \to \min$ whenever $g(F) \to \max$.

From figure C1 we see that $g(F) \to \max$ for $F \to \min$. This implies for (C12) that

$$p_1 \leqslant 2\exp\left\{\frac{-n}{a(F)}\left[(g(F_{\min})+\delta)\log\left(1+\frac{\delta}{g(F_{\min})}\right)-\delta\right]\right\}. \tag{C14}$$

Consequently $(g(F_{\min})+\delta)\log\left(1+\frac{\delta}{g(F_{\min})}\right)-\delta \geqslant 0$ and $a(F) \leqslant a(F_{\max})$ implies

$$p_1 \leqslant 2\exp\left\{\frac{-n}{a_{\max}}\left[(g_{\max}+\delta)\log\left(1+\frac{\delta}{g_{\max}}\right)-\delta\right]\right\}, \tag{C15}$$

where $a_{\max} = a(F_{\max})$ and $g_{\max}=g(F_{\min})$. We rewrite (C15) in a more compact form by defining $x_1(\delta) = 1/a_{\max}\left[(g_{\max}+\delta)\log\left(1+\frac{\delta}{g_{\max}}\right)-\delta\right]$ and inserting $\delta = n^{-1/5}$ [9] as

$$p_1 \leqslant 2\exp(-nx_1(n^{-1/5})). \tag{C16}$$

We will use (C16) for the confidentiality estimate (C8). In order to show that (C16) ensures an exponential convergence, as we claim, we need to provide an upper bound for the exponent of (C16), i.e. for the function

$$-\frac{n}{a_{\max}}\left[(g_{\max}+\delta)\log\left(1+\frac{\delta}{g_{\max}}\right)-\delta\right] \tag{C17}$$

[9] The choice of δ is a trade-off between the rate of convergence and the number of output system $m = n(1 - S(\rho) - 2\delta)$. Any choice $\delta < n^{-1/4}$ is appropriate.

where δ will be choosen later as $n^{-1/5}$ as previously. By defining

$$f(n) = n\left((g_{\max}+\delta)\log\left(1+\frac{\delta}{g_{\max}}\right)-\delta\right). \tag{C18}$$

Equation (C17) reads as $-f(n)/a_{\max}$. In the following we compute a lower bound $y(n)$ for $f(n)$, i.e. $f(n) > y(n)$ for all n, which is in turn an upper bound for (C16), i.e. $p_1 \leqslant 2\exp(-f(n)/a_{\max}) \leqslant 2\exp(-y(n)/a_{\max})$. Using that $\log(1+x) > \frac{x}{1+x/2}$ for $x > 0$, see [59], we find from $g_{\max}>0$ and $\delta > 0$ that

$$\log\left(1+\frac{\delta}{g_{\max}}\right) > \frac{\frac{\delta}{g_{\max}}}{1+\frac{\delta}{2g_{\max}}} = \frac{2\delta}{2g_{\max}+\delta}. \tag{C19}$$

Furthermore we have that $(g_{\max}+\delta)\log\left(1+\frac{\delta}{g_{\max}}\right)-\delta \geqslant 0$ which implies together with (C19) for (C18)

$$\begin{aligned} f(n) &> n\left((g_{\max}+\delta)\frac{2\delta}{2g_{\max}+\delta}-\delta\right) \\ &= n\frac{2\delta(g_{\max}+\delta)-(2g_{\max}+\delta)\delta}{2g_{\max}+\delta} \\ &= n\frac{2\delta g_{\max}+2\delta^2-2g_{\max}\delta-\delta^2}{2g_{\max}+\delta} \\ &= \frac{n\delta^2}{2g_{\max}+\delta} \geqslant \frac{n\delta^2}{2g_{\max}+1} \end{aligned} \tag{C20}$$

because $\delta \leqslant 1$. Inserting $\delta = n^{-1/5}$ finally gives

$$f(n) > \frac{n\delta^2}{2g_{\max}+1} = \frac{n^{3/5}}{2g_{\max}+1} =: y(n) \tag{C21}$$

implying

$$p_1 \leqslant 2\exp(-f(n)/a_{\max}) \leqslant 2\exp(-y(n)/a_{\max}) = 2\exp\left(-\frac{n^{3/5}}{a_{\max}(2g_{\max}+1)}\right) \tag{C22}$$

which analytically proves the exponential scaling of the hashing protocol.

Furthermore, following the approach of [29], we find that the probability of having two configurations which are compatible with the collected parity information, p_2, is bounded by $2^{-n\delta}$. Thus, inserting $\delta = n^{-1/5}$ gives $p_2 < 2^{-n^{4/5}}$.

Finally we provide an estimate for the probability of accepting initial states from Eve in the case when Alice and Bob should abort the protocol after parameter estimation, i.e. the actual fidelity F is below the minimum required value $F_{\min}$ but the estimate $\overline{F}$ is not, or the actual fidelity F is above $F_{\max}$ but the estimate $\overline{F}$ is not, corresponding to the probability p_3'. For that purpose we perform two-qubit measurements of two Bell-pairs, the first w.r.t. the $X\otimes X$ and the second w.r.t. the $Z\otimes Z$ observable. One easily observes that $|B_{00}\rangle$ is the common $+1$ eigenstate of both operators. By referring to this measurements as M_1 and M_2 respectively and recalling that the parameter estimation utilizes kn systems we define the random variables F_i associated with a pair of Bell-pairs for $1 \leqslant i \leqslant kn/2$ which is equal to 1 whenever M_1 and M_2 simultaneously reveal outcome 1 and 0 otherwise. Recall that the Hoeffding inequality [60] states that we have for X_1 ,..., X_n i.i.d. random variables where $a_i \leqslant X_i \leqslant b_i$, $c_i = b_i - a_i$, $S_n = \sum_i X_i$ and the expected value E_n of S_n, i.e. $E_n = E[S_n]$, that

$$\Pr(|S_n - E_n| > t) < 2\exp\left(-\frac{2t^2}{nC^2}\right) \tag{C23}$$

holds for all t and where $\forall i$: $c_i \leqslant C$. Hoeffding's inequality (C23) implies now for the empirical mean $\overline{F} = 2\Big/(kn)\sum_{i=1}^{kn/2} F_i$ that

$$\Pr(|\overline{F} - E[F]| > \eta) < 2\exp(-\eta^2 kn) \tag{C24}$$

holds for all η. More precisely, the probability of estimating an error larger than η via $\overline{F}$ to $E[F]$ is decaying exponential in n. So Alice and Bob choose $F_{\min}$ and $F_{\max}$ and they agree to continue with the hashing protocol whenever $\overline{F} \in [F_{\rm PE} - \Delta/4, F_{\rm PE} + \Delta/4]$ where $F_{\rm PE} = (F_{\min} + F_{\max})/2$ and $\Delta = F_{\max} - F_{\min}$. Fixing $\eta = \Delta/4$ implies for (C24) that

$$\Pr(|\overline{F} - E[F]| > \eta) < 2\exp(-(F_{\max} - F_{\min})^2 kn/16). \tag{C25}$$

In other words, (C25) means that the probability that Alice and Bob continue with the hashing protocol in case they should abort, i.e. the actual fidelity F is outside $[F_{\min}, F_{\max}]$, is exponentially small. For example, if the fidelity estimate $\overline{F}$ is $\overline{F} = F_{\mathrm{PE}} + \Delta/4$ (which implies Alice and Bob will run hashing), then the probability that the actual fidelity F satisfies $F > F_{\mathrm{PE}} + \Delta/2 = F_{\max}$ is exponentially bounded.

To summarize, we find for (C2) that

$$\|\mathcal{E}(\rho^{\otimes n+kn}) - \mathcal{F}(\rho^{\otimes n+kn})\|_1 \leqslant 2[2\exp(-nx_1(n^{-1/5})) + \exp(-n^{4/5}\ln 2) + 2\exp(-(F_{\max} - F_{\min})^2 kn/16)]. \tag{C26}$$

Notice that the right-hand side of (C26) is independent of ρ, which completes the proof. □

Appendix D. Local closeness implies global closeness

In the main text we formulated the following claim: if the output of the real and ideal map differ at most ε for a particular initial state then they differ at most $4\sqrt{\varepsilon}$ for any purification of this initial state. We prove this statement within the following Lemma.

Lemma 1. *Let $\mathcal{E}$ be the real and $\mathcal{F}$ be the ideal protocol. Furthermore let ρ be a mixed state shared by the participants of the protocol. If $\|\mathcal{E}(\rho) - \mathcal{F}(\rho)\|_1 \leqslant \varepsilon$, then*

$$\|(\mathcal{E}\otimes \mathrm{id}_E - \mathcal{F}\otimes \mathrm{id}_E)(|\psi\rangle\langle\psi|_{ABE})\|_1 \leqslant 4\sqrt{\varepsilon} \tag{D1}$$

for all purifications $|\psi\rangle_{ABE}$ of ρ.

Proof. We observe that

$$\mathcal{E}(\rho) = p_\rho \sigma_{AB}\otimes |\mathrm{ok}\rangle\langle \mathrm{ok}| + (1-p_\rho)\sigma^{\perp}_{AB}\otimes |\mathrm{fail}\rangle\langle \mathrm{fail}|, \tag{D2}$$

$$\mathcal{F}(\rho) = p_\rho |\varphi\rangle\langle\varphi|^{\otimes m}_{AB}\otimes |\mathrm{ok}\rangle\langle \mathrm{ok}| + (1-p_\rho)\sigma^{\perp}_{AB}\otimes |\mathrm{fail}\rangle\langle \mathrm{fail}|. \tag{D3}$$

The assumption $\|\mathcal{E}(\rho) - \mathcal{F}(\rho)\|_1 \leqslant \varepsilon$ implies $p_\rho\|\sigma_{AB} - |\varphi\rangle\langle\varphi|^{\otimes m}_{AB}\|_1 \leqslant \varepsilon$ because $\mathcal{E}(\rho)$ and $\mathcal{F}(\rho)$ are equal on the fail branch. Thus we have $\|\sigma_{AB} - |\varphi\rangle\langle\varphi|^{\otimes m}_{AB}\|_1 \leqslant \varepsilon/p_\rho$.

Furthermore we find for the application of the real and the ideal protocol to a purification $|\psi\rangle_{ABE}$ of ρ_{AB} that

$$(\mathcal{E}\otimes \mathrm{id}_E)(|\psi\rangle\langle\psi|_{ABE}) = p_\rho \sigma_{ABE}\otimes |\mathrm{ok}\rangle\langle \mathrm{ok}| + (1-p_\rho)\sigma^{\perp}_{ABE}\otimes |\mathrm{fail}\rangle\langle \mathrm{fail}|, \tag{D4}$$

$$(\mathcal{F}\otimes \mathrm{id}_E)(|\psi\rangle\langle\psi|_{ABE}) = p_\rho |\varphi\rangle\langle\varphi|^{\otimes m}_{AB}\otimes \rho_E\otimes |\mathrm{ok}\rangle\langle \mathrm{ok}| + (1-p_\rho)\sigma^{\perp}_{ABE}\otimes |\mathrm{fail}\rangle\langle \mathrm{fail}|. \tag{D5}$$

This implies for the one-norm that

$$\begin{aligned}&\|(\mathcal{E}\otimes \mathrm{id}_E - \mathcal{F}\otimes \mathrm{id}_E)(|\psi\rangle\langle\psi|_{ABE})\|_1\\ &= p_\rho\|\sigma_{ABE} - |\varphi\rangle\langle\varphi|^{\otimes m}_{AB}\otimes\rho_E\|_1.\end{aligned} \tag{D6}$$

Thus we need to show that $p_\rho\|\sigma_{ABE} - |\varphi\rangle\langle\varphi|^{\otimes m}_{AB}\otimes\rho_E\|_1 \leqslant 4\sqrt{\varepsilon}$. One easily verifies $\mathrm{tr}_E[\sigma_{ABE}] = \sigma_{AB}$ and $\mathrm{tr}_{AB}[\sigma_{ABE}] = \rho_E$ because the system E is not affected by the protocol $\mathcal{E}$. Recall that we have by assumption that $\|\sigma_{AB} - |\varphi\rangle\langle\varphi|^{\otimes m}_{AB}\|_1 \leqslant \varepsilon/p_\rho$. Thus we apply lemma 10 of the supplementary material from [28] to $\rho_{SE} := \sigma_{ABE}$ and $\varphi_{SE} := |\varphi\rangle\langle\varphi|^{\otimes m}_{AB}\otimes\rho_E$ where $S := AB$ which implies

$$\|\sigma_{ABE} - |\varphi\rangle\langle\varphi|^{\otimes m}_{AB}\otimes\rho_E\|_1 \leqslant 4\sqrt{\varepsilon/p_\rho}. \tag{D7}$$

Employing (D7) in (D6) yields

$$\|(\mathcal{E}\otimes \mathrm{id}_E - \mathcal{F}\otimes \mathrm{id}_E)(|\psi\rangle\langle\psi|_{ABE})\|_1 \leqslant p_\rho 4\sqrt{\varepsilon/p_\rho} = 4\sqrt{p_\rho\varepsilon} \leqslant 4\sqrt{\varepsilon} \tag{D8}$$

which completes the proof. □

Appendix E. Proof of theorem 1

Proof. Due to the symmetrization we find that $\mathcal{E}^s$ and $\mathcal{F}^s$ are permutation invariant maps. Hence applying the post-selection technique of [46] gives

$$\|\mathcal{E}^s - \mathcal{F}^s\|_\diamond \leqslant g_{n+kn,d}\|(\mathcal{E}^s\otimes \mathrm{id}_E - \mathcal{F}^s\otimes \mathrm{id}_E)(|\tau\rangle\langle\tau|_{ABE})\|_1, \tag{E1}$$

where d is determined by the number of participants (see the main text) and $|\tau\rangle_{ABE}$ is a purification of the de-Finetti Hilbert–Schmidt state, hence $\mathrm{tr}_E[|\tau\rangle\langle\tau|_{ABE}] = \int\sigma^{\otimes n+kn}_{AB}\mathrm{d}\mu(\sigma) =: \tau'$ where μ is the measure induced by the Hilbert–Schmidt metric on $\mathrm{End}(\mathbb{C}^d)$. One easily observes that

$$\|\mathcal{E}^s(\tau') - \mathcal{F}^s(\tau')\|_1 = \left\|(\mathcal{E}^s - \mathcal{F}^s)\left(\int \sigma_{AB}^{\otimes n+kn} \mathrm{d}\mu(\sigma)\right)\right\|_1 \leqslant \max_{\sigma_{AB}} \|(\mathcal{E} - \mathcal{F})(\sigma_{AB}^{\otimes n+kn})\|_1, \tag{E2}$$

where $\mathcal{E}$ and $\mathcal{F}$ denote the subprotocols after symmetrization. As $|\tau\rangle_{ABE}$ is a purification of τ' we can apply lemma 1 implying for (E1) that

$$\begin{aligned}
&\|\mathcal{E}^s - \mathcal{F}^s\|_\diamond \\
&\leqslant g_{n+kn,d} \|(\mathcal{E}^s \otimes \mathrm{id}_E - \mathcal{F}^s \otimes \mathrm{id}_E)(|\tau\rangle\langle\tau|_{\mathrm{ABE}})\|_1 \\
&\leqslant g_{n+kn,d} 4\sqrt{\|(\mathcal{E}^s - \mathcal{F}^s)(\mathrm{tr}_E[|\tau\rangle\langle\tau|_{\mathrm{ABE}}])\|_1} \\
&= 4g_{n+kn,d}\sqrt{\|(\mathcal{E}^s - \mathcal{F}^s)(\tau')\|_1} \\
&\leqslant 4g_{n+kn,d}\sqrt{\max_{\sigma_{AB}} \|(\mathcal{E} - \mathcal{F})(\sigma_{AB}^{\otimes n+kn})\|_1},
\end{aligned} \tag{E3}$$

where the second inequality stems from lemma 1 and the last inequality from (E2) which finally shows the claim. □

Appendix F. Confidentiality of a noisy measurement-based implementation of the hashing protocol

Within this section we prove equation (8) of the main text. In doing so, we formulate the following Theorem.

Theorem 3. *Let $\mathcal{E}^{s,\alpha}$ and $\mathcal{F}^{s,\alpha}$ be the real and the ideal noisy hashing protocol prepended by symmetrization where noise of strength $1-\alpha$ of the form (A1) acts on each qubit of the resource states independent and identical. Then*

$$\|\mathcal{E}^{s,\alpha} - \mathcal{F}^{s,\alpha}\|_\diamond \leqslant \|\mathcal{E}^s - \mathcal{F}^s\|_\diamond. \tag{F1}$$

Proof. The resource state each protocol party requires for the measurement-based implementation of hashing is pure, minimal in the number of qubits and consists only of input and output qubits, because all quantum gates involved in the hashing protocol are elements of the Clifford group [41].

Hence there are only two different locations at which noise acts: input and output qubits. For the noise acting on the input qubits we use the observation made in [42], which enables us to *virtually* move the noise from the input qubits to the initial states, thereby increasing their entropy. For the noise acting on the output qubits, as described in the main text, we can safely assume that this noise will act after the protocol completes, leaving us with a noiseless hashing protocol (w.r.t. the output qubits).

We deal with the noise on the input qubits by a slight modification of the parameter estimation step. Recall that Alice and Bob fix $F_{\min}$ and $F_{\max}$ for parameter estimation and they continue with the hashing protocol whenever their fidelity estimate $\overline{F}$ is within the interval $[F_-, F_+]$ where $F_\pm = F_{\mathrm{PE}} \pm \Delta/4$ for $F_{\mathrm{PE}} = (F_{\max} + F_{\min})/2$ and $\Delta = F_{\max} - F_{\min}$. The noise acting on the input qubits of the resource states increases the entropy of the initial states which forces Alice and Bob to accept less initial states from Eve. By describing the initial states in an i.i.d. setting after the twirl via i.i.d. LDN of the form (A1), i.e. $\rho = D_1(q)|B_{00}\rangle\langle B_{00}|$, the parameter estimation interval $[F_-, F_+]$ transforms to $[q_-, q_+]$ via $q_\pm = (4F_\pm - 1)/3$. According to the previous observation that we can virtually move the noise of level α on the input qubits of the resource states, $D_1(\alpha)$ and $D_2(\alpha)$ respectively, to the initial states we consequently describe the initial states as $D_2(\alpha)D_1(\alpha)D_1(q)|B_{00}\rangle\langle B_{00}| = D_1(\alpha^2)D_1(q)|B_{00}\rangle\langle B_{00}| = D_1(\alpha^2 q)|B_{00}\rangle\langle B_{00}|$, see also figure F1. Observe that we have moved the noise from Bob's to Alice's side due to the symmetry of Bell-states. Thus we need to have $\alpha^2 q \in [q_-, q_+]$ to pass the parameter estimation and run the hashing protocol. Observe that $\alpha^2 q$ transforms to the fidelity F' of the initial states, including the noise of the resource state, via $\alpha^2 q = (4F' - 1)/3$. Therefore we modify the parameter estimation to continue with the hashing protocol whenever the estimate of the fidelity $\overline{F}$ of the initial states satisfies

$$\overline{F} \in \left[\frac{3q_- + \alpha^2}{4\alpha^2}, \frac{3q_+ + \alpha^2}{4\alpha^2}\right], \tag{F2}$$

see figure F2.

We denote the protocols with modified parameter estimation according to condition (F2) by the maps $\mathcal{E}^{s,\alpha\text{-in}}$ and $\mathcal{F}^{s,\alpha\text{-in}}$ respectively. It follows immediately from the definition of the protocols that we achieve the same confidentiality level of equation (7) of the main text as for the noiseless protocols, Alice and Bob will just abort the protocol more often. Hence we easily deduce

$$\|\mathcal{E}^{s,\alpha\text{-in}} - \mathcal{F}^{s,\alpha\text{-in}}\|_\diamond = \|\mathcal{E}^s - \mathcal{F}^s\|_\diamond. \tag{F3}$$

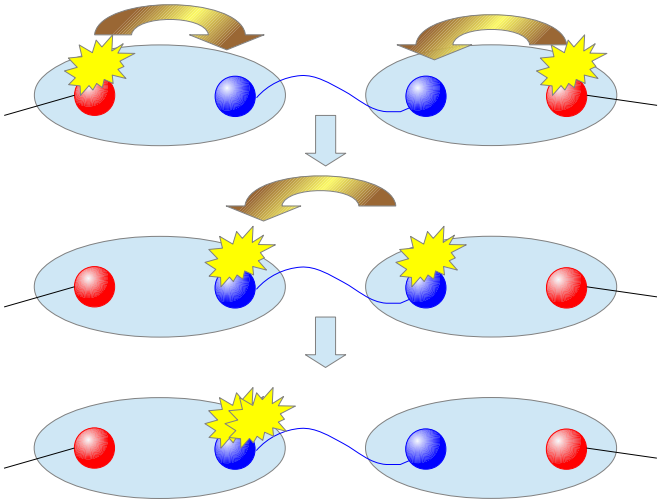

Figure F1. The figure shows, at an abstract level, how noise on the input qubits is moved from the resource states to the initial states. The blue ellipsis indicate Bell-measurements, the red vertices the input qubits of the resource state and the light-blue vertices the qubits of the initial states.

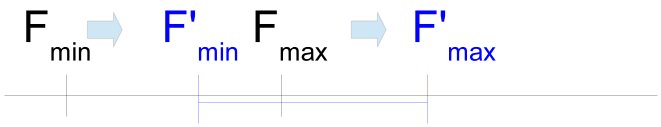

Figure F2. The interval for parameter estimation acceptance $[F_{\min}, F_{\max}]$ transforms according to (F2) to $[F'_{\min}, F'_{\max}]$.

We now extend the confidentiality proof to a full noisy measurement-based implementation of the hashing protocol protocol as follows: since we can effectively move noise of level α acting on the input qubits of the resource states to the to-be-purified ensemble, the modification (F2) of the parameter estimation extends the confidentiality proof via (F3) to noise acting on the input qubits of the resource state. For noise acting on the output qubits we use the following observation: Because the noise is assumed to be of the form (A1) it is also CPTP. By denoting the noise acting on the output qubits as $\mathcal{N}^{\alpha} = \bigotimes_{j=1}^{m} \mathcal{D}_{j;A}(\alpha)\mathcal{D}_{j;B}(\alpha)$ where A and B denote Alice's and Bob's parts of the final Bell-pairs, the noisy real protocol and ideal protocol read as $\mathcal{E}^{s,\alpha} = \mathcal{N}^{\alpha}\circ\mathcal{E}^{s,\alpha\text{-in}}$ and $\mathcal{F}^{s,\alpha} = \mathcal{N}^{\alpha}\circ\mathcal{F}^{s,\alpha\text{-in}}$ respectively[10]. Hence (F3) and the contractivity of the 1- norm for CPTP maps imply

$$\|\mathcal{E}^{s,\alpha} - \mathcal{F}^{s,\alpha}\|_{\diamondsuit} = \|\mathcal{N}^{\alpha}\circ(\mathcal{E}^{s,\alpha\text{-in}} - \mathcal{F}^{s,\beta\text{-in}})\|_{\diamondsuit} \leqslant \|\mathcal{E}^{s,\alpha\text{-in}} - \mathcal{F}^{s,\alpha\text{-in}}\|_{\diamondsuit} = \|\mathcal{E}^{s} - \mathcal{F}^{s}\|_{\diamondsuit}. \tag{F4}$$

What remains to be dealt with are the Pauli byproduct operators due to the measurement outcomes at the inputs, but since LDN of the form (A1) commutes with the Pauli byproduct operators we do not have to worry about them in the proof of confidentiality, which completes the proof. □

Appendix G. Confidentiality of multiparty hashing protocol for two-colorable graph states

We start by recalling some basic notation, definitions and properties of graph states.

We define the graph state basis $|\psi_{\kappa_1,\ldots,\kappa_N}\rangle$ where $\kappa_1,\ldots,\kappa_N \in \{0, 1\}$ associated with a graph $G = (V, E)$ where $N = |V|$ as the common eigenstate of the correlation operators

$$K_j = X^{(j)} \prod_{\{j,k\}\in E} Z^{(k)} \tag{G1}$$

with eigenvalues $(-1)^{\kappa_j}$ for $1 \leqslant j \leqslant N$ where the superscript denotes the qubit on which the Pauli operator is acting on. We refer to the state $|\psi_{0,\ldots,0}\rangle$ also as the graph state associated with $G = (V, E)$. Note that the states $\{|\psi_{\kappa_1,\ldots,\kappa_N}\rangle\}_{\kappa_1,\ldots,\kappa_N=0}^{1}$ form a basis of the Hilbert-space $(\mathbb{C}^2)^{\otimes N}$. A special class of graph states are so-called two-colorable graph states which correspond to two-colorable graphs. A graph is said to be two-colorable if there

[10] This is due to the fact that we can assume that the noise acting on the output qubits is applied after the protocol(s) have finished.

exists a mapping $f\colon V \to \{1, 2\}$ such that for all vertices $v \in V$ it holds that $f(v) \neq f(w)$ for all neighbors $w \in V$ of v. The most prominent examples of two-colorable graph states are GHZ and cluster states [54].

Suppose we want to distill a two-colorable graph state $|\psi_{0\ldots0}\rangle$ corresponding to a graph $G = (V, E)$ where $V = V_A \cup V_B$, A and B denote the colors and $|V_A| = N_A$, $|V_B| = N_B$ where $N = N_A + N_B$. The multipartite hashing protocol assumes asymptotically many i.i.d. initial states ρ diagonal in the graph state basis, i.e. $\rho = \sum_{\boldsymbol{\mu},\boldsymbol{\nu}} \lambda_{\boldsymbol{\mu},\boldsymbol{\nu}} |\psi_{\boldsymbol{\mu},\boldsymbol{\nu}}\rangle\langle\psi_{\boldsymbol{\mu},\boldsymbol{\nu}}|$ where $\boldsymbol{\mu} = (\mu_1,\ldots,\mu_{N_A}) \in \{0, 1\}^{N_A}$ and $\boldsymbol{\nu} = (\nu_1,\ldots,\nu_{N_B}) \in \{0, 1\}^{N_B}$ are multi-indices corresponding to color A and B respectively[11] .For two-colorable graph states we define multilateral CNOTs on two copies ρ_1 and ρ_2 which enable us to transfer information between the initial states ρ_1 and ρ_2. More precisely, by applying a CNOT to all particles in V_A (V_B) where ρ_1 serves as target(source) and ρ_2 as source (target) a straightforward computation leads to (by denoting this unitary as U_1)

$$|\psi_{\boldsymbol{\mu},\boldsymbol{\nu}}\rangle \otimes |\psi_{\boldsymbol{\mu}',\boldsymbol{\nu}'}\rangle \xrightarrow{U_1} |\psi_{\boldsymbol{\mu},\boldsymbol{\nu}\oplus\boldsymbol{\nu}'}\rangle \otimes |\psi_{\boldsymbol{\mu}\oplus\boldsymbol{\mu}',\boldsymbol{\nu}'}\rangle. \tag{G2}$$

By exchanging the roles of V_A and V_B one obtains (by denoting this unitary as U_2)

$$|\psi_{\boldsymbol{\mu},\boldsymbol{\nu}}\rangle \otimes |\psi_{\boldsymbol{\mu}',\boldsymbol{\nu}'}\rangle \xrightarrow{U_2} |\psi_{\boldsymbol{\mu}\oplus\boldsymbol{\mu}',\boldsymbol{\nu}}\rangle \otimes |\psi_{\boldsymbol{\mu}',\boldsymbol{\nu}\oplus\boldsymbol{\nu}'}\rangle. \tag{G3}$$

Suppose we measure all qubits of the graph state $|\psi_{\mu_1,\ldots,\mu_{N_A},\nu_1,\ldots,\nu_{N_B}}\rangle$ belonging to the set V_A with the X and all qubits of the set V_B with the Z observable. By denoting the outcomes of the X measurements with $\xi_i \in \{0, 1\}$ and the outcomes of the Z measurements with $\zeta_j \in \{0, 1\}$ one immediately finds via (G1)

$$\mu_i = \left(\xi_i + \sum_{\{i,j\}\in E} \zeta_j\right) \bmod 2 \tag{G4}$$

for all $1 \leqslant i \leqslant N_A$. In other words, we can use this measurement setting to reveal information about all κ_i for $1 \leqslant i \leqslant N_A$ simultaneously. We refer to this measurements with M_1. Similarly, by exchanging the roles of V_A and V_B we obtain information about all ν_i for $1 \leqslant i \leqslant N_B$. In the following, we refer to this measurements with M_2.

The multiparty hashing protocol is now defined as follows [30]: in order to reveal information about color A, i.e. $\boldsymbol{\mu}$, (which we denote as sub-protocol P_1) we apply U_1 to a random subset of the n initial states with a common target system (thereby accumulating the values corresponding to color A) and perform measurement M_1 on this common system. Similarly, by applying U_2 to a random subset of the initial states with a common target system (thereby accumulating the values corresponding to color B) followed by M_2 on this common system one obtains information about color B, i.e. $\boldsymbol{\nu}$ (which we denote as sub-protocol P_2). Repeating the sub-protocols P_1 and P_2 sufficiently many times leads to perfect knowledge about the remaining states, i.e. one ends up in a pure state (which we can restore to the target state $|\psi_{0,\ldots,0}\rangle^{\otimes m}$).

Recall that the overall protocol prepends the multiparty hashing protocol by a twirling and parameter estimation step. The twirling step ensures that the initial states are diagonal within the graph state basis, see [30], whereas the participants use parameter estimation to decide whether the multiparty hashing protocol will succeed or not.

Formally, we define the probabilities

$$a_i^{(\mu_i)} = \sum_{\mu_k\neq\mu_j,\nu} \lambda_{\mu_1,\ldots,\mu_i,\ldots,\mu_{N_A},\nu}, \tag{G5}$$

$$b_j^{(\nu_j)} = \sum_{\nu_k\neq\nu_j,\mu} \lambda_{\mu,\nu_1,\ldots,\nu_j,\ldots,\nu_{N_B}} \tag{G6}$$

for $1 \leqslant i \leqslant N_A$ and $1 \leqslant j \leqslant N_B$. For example, for a three-qubit state we have $a_1^{(0)} = \sum_{k,l}\lambda_{0kl}$ and $a_1^{(1)} = \sum_{k,l}\lambda_{1kl}$. Observe that the values $S(a_i)$ and $S(b_j)$ correspond to the entropies of μ_i and ν_j within the vectors $\boldsymbol{\mu}$ and $\boldsymbol{\nu}$.

As shown in [30], the protocol described above is capable of distilling $m = n(1 - \max_{1\leqslant i\leqslant N_A} S(a_i) - \max_{1\leqslant j\leqslant N_B} S(b_j))$ copies of the state $|\psi_{0,\ldots,0}\rangle$ in the asymptotic limit.

Now we are ready to compute the distance of the real and ideal multiparty hashing protocol for i.i.d. initial states. Intuitively it follows from the same arguments as in the bipartite setting.

Theorem 4. *Let $\mathcal{E}$ be the real and $\mathcal{F}$ be the ideal multiparty hashing protocol. Furthermore let ρ be an initial state. Then*

$$\|\mathcal{E}(\rho^{\otimes n+kn}) - \mathcal{F}(\rho^{\otimes n+kn})\|_1 \leqslant \varepsilon_{\mathrm{H}}, \tag{G7}$$

where $\varepsilon_{\mathrm{H}} \in O(\exp(-\sqrt{n}))$ is independent of the initial state ρ.

[11] If the initial states are not diagonal in the graph state basis we achieve this by probabilistically applying the correlation operators (G1), see [30]. This procedure is also referred to as twirling.

Proof. Recall that the multiparty hashing protocol aims to distill several copies of a two-colorable graph state via the sub-protocols P_1 for color A and P_2 for color B from n copies of the initial state $\rho = \sum_{\boldsymbol{\mu},\boldsymbol{\nu}} |\psi_{\boldsymbol{\mu},\boldsymbol{\nu}}\rangle \langle\psi_{\boldsymbol{\mu},\boldsymbol{\nu}}|$ where the states $|\psi_{\boldsymbol{\mu},\boldsymbol{\nu}}\rangle$ correspond to the graph state basis.

The crucial observation is that we learn the values of $\boldsymbol{\mu}$ and $\boldsymbol{\nu}$ corresponding to the colors A and B within n copies of the initial state $\rho = \sum_{\boldsymbol{\mu},\boldsymbol{\nu}} |\psi_{\boldsymbol{\mu},\boldsymbol{\nu}}\rangle \langle\psi_{\boldsymbol{\mu},\boldsymbol{\nu}}|$ via the sub-protocols P_1 and P_2 independently. In other words, $\boldsymbol{\mu}$ and $\boldsymbol{\nu}$ do not get correlated during the protocol execution, i.e. they remain independent. By taking a closer look at P_1 (P_2) we infer that also the individual components of $\boldsymbol{\mu}$ ($\boldsymbol{\nu}$) remain independent. In particular, the components of $\boldsymbol{\mu} = (\mu_1,\ldots, \mu_{N_A})$ ($\boldsymbol{\nu} = (\nu_1,\ldots, \nu_{N_B})$) remain distinct during the protocol, i.e. for each i the value μ_i is independent of μ_k for all $k \neq i$ (for each j the value ν_j is independent of ν_k for all $k \neq j$). This is due to the fact that U_1 (U_2) operates component-wise on $\boldsymbol{\mu}$ ($\boldsymbol{\nu}$) [12]. Keeping this observations in mind, it is straightforward to provide finite size estimates for the fidelity of the state after the protocol relative to $|\psi_{0,\ldots,0}\rangle$. Observe that the hashing protocol fails if either P_1 or P_2 fails which implies for the failure probability p_f of the hashing protocol that $p_f \leqslant p_{P_1} + p_{P_2}$ where p_{P_1} and p_{P_2} denote the failure probabilities of sub-protocol P_1 and P_2 respectively.

First we discuss the failure probability of sub-protocol P_1. This sub-protocol can fail due to three reasons, similar as in the bipartite setting: the initial states do not belong to the likely subspace or, after the sub-protocol has finished, two or more configurations are compatible with the collected parity information, or the protocol is continued mistakenly after parameter estimation, i.e. the parties should have aborted but continued the multiparty hashing protocol to its very end.

To provide an estimate for the probability that the initial states fall outside the likely subspace w.r.t. sub-protocol P_1 we define for color A the random variables $X^{(i)}(b)$ for $1 \leqslant i \leqslant N_A$ which take the values

$$X^{(i)}(b) = -\log_2 a_i^{(b)} - S(a_i) \tag{G8}$$

with probability $a_i^{(b)}$. In order to learn $\boldsymbol{\mu}$, we observe that a specific $\boldsymbol{\mu} = (\mu_1,\ldots, \mu_{N_A})$ belongs to the likely subspace $\mathcal{L}$ whenever each μ_i belongs to its likely subspace $\mathcal{L}_i$, i.e.

$$\boldsymbol{\mu} \in \mathcal{L} \Leftrightarrow \forall\, 1 \leqslant i \leqslant N_A\colon\ \mu_i \in \mathcal{L}_i. \tag{G9}$$

Consequently,

$$\Pr(\boldsymbol{\mu} \notin \mathcal{L}) \leqslant \sum_{i=1}^{N_A} \Pr(\mu_i \notin \mathcal{L}_i) \leqslant N_A \max_{1\leqslant i\leqslant N_A} \Pr(\mu_i \notin \mathcal{L}_i). \tag{G10}$$

We estimate $\Pr(\mu_i \notin \mathcal{L}_i)$ via Hoeffding's inequality [60]. In order to apply Hoeffding's inequality we need to make sure that $\lambda_{\boldsymbol{\mu},\boldsymbol{\nu}} \neq 0$ for all $\boldsymbol{\mu}$ and $\boldsymbol{\nu}$ after twirling, as the the random variables $X^{(i)}(b)$ of (G8) need to be bounded. We achieve this by mixing each individual initial state with a small, but defined, portion of the identity operator. From this we observe that the random variables $X^{(i)}$ have zero mean and that $|X^{(i)}| \leqslant \max_{b\in 0,1} |\log_2 a_i^{(b)}| + S(a_i) =: C_i$ after mixing. Therefore the Hoeffding inequality implies

$$\Pr\left(\left|\sum_{k=1}^{n} X_k^{(i)}\right| > t\right) \leqslant 2\exp\left(\frac{-2t^2}{nC_i^2}\right) \tag{G11}$$

for all t where k denotes the index of the initial state within $\rho^{\otimes n}$ and i the ith component of $\boldsymbol{\mu}$. Inserting $t = n\delta$ in (G11) together with $\delta = n^{-1/4}$ yields

$$\begin{aligned}\Pr(\mu_i \notin \mathcal{L}_i) = \Pr\left(\left|\sum_{k=1}^{n} X_k^{(i)}\right| > n^{3/4}\right) &\leqslant 2\exp\left(\frac{-2\sqrt{n}}{C_i^2}\right)\\ &\leqslant 2\exp\left(\frac{-2\sqrt{n}}{C^2}\right),\end{aligned} \tag{G12}$$

where $C = \max_{1\leqslant i\leqslant N_A} C_i$. Note that (G12) is independent of i, which implies for (G10) that

$$\Pr(\boldsymbol{\mu} \notin \mathcal{L}) \leqslant 2N_A \exp\left(\frac{-2\sqrt{n}}{C^2}\right). \tag{G13}$$

Observe that $C = \max_{1\leqslant i\leqslant N_A} C_i$ still depends on the initial states. Due to parameter estimation one finds another constant $C' > C$ independent of the initial states. The probability of not being able to distinguish between two or more configurations is, for a particular component of $\boldsymbol{\mu}$, again $2^{-n\delta}$, as for the bipartite case. Hence inserting $\delta = n^{-1/4}$ gives that the probability of misidentifying a specific μ_i where $1 \leqslant i \leqslant N_A$ is bounded by $2^{-n^{3/4}}$. Therefore the probability of misidentifying $\boldsymbol{\mu}$ is bounded by $N_A 2^{-n^{3/4}}$.

We point out that also in the multipartite setting a parameter estimation step is crucial in order to ensure entanglement distillation. For that purpose we find that the states after twirling and mixing are diagonal within the graph state basis, i.e. of the form

[12] Intuitively speaking this independence stems from the two-colorability of the graph-state and the properties of U_1 and U_2.

$$\rho = \sum_{\mu,\nu} \lambda_{\mu,\nu} |\psi_{\mu,\nu}\rangle \langle \psi_{\mu,\nu}|, \tag{G14}$$

where all $\lambda_{\mu,\nu} \neq 0$. The goal of parameter estimation is to provide estimates $\overline{a_i}$ and $\overline{b_j}$ for the probability distributions a_i and b_j of (G5) and (G6) for all $1 \leqslant i \leqslant N_A$ and $1 \leqslant j \leqslant N_B$. The concrete boundaries for which the participants continue with hashing depends on the target state of the protocol. However, it suffices to estimate $\lambda_{\mu,\nu}$ for all $\boldsymbol{\mu}$ and $\boldsymbol{\nu}$ which we denote by $\overline{\lambda_{\mu,\nu}}$. Observe that we have to determine in total 2^N coefficients, where N denotes the number of participants and is constant. This can be done via measurements on kn systems of ρ according to the observables of the correlation operators (G1). Indeed, the expected values of the correlation operators are sufficient to determine the coefficients $\lambda_{\mu,\nu}$ for all $\boldsymbol{\mu}$ and $\boldsymbol{\nu}$ within $\rho = \sum_{\mu,\nu} \lambda_{\mu,\nu} |\psi_{\mu,\nu}\rangle \langle \psi_{\mu,\nu}|$. Now one can apply Hoeffding's inequality to exponentially bound the probabilities that the estimates $\overline{\lambda_{\mu,\nu}}$ of $\lambda_{\mu,\nu}$ have a distance larger than some fixed $\eta > 0$ (which corrsponds to the accuracy of our estimate $\overline{\lambda_{\mu,\nu}}$) similar to the bipartite case. From this we deduce that the probability of continuing with the hashing protocol mistakenly is exponentially small in terms of the number n of initial states.

In summary, via the same argument as in the bipartite case (i.e. the previous estimates are upper bounds for the real failure probabilities, see (C3), (C4) and (C8)), the probability that sub-protocol P_1 fails satisfies $p_{P_1} \in O(\exp(-\sqrt{n}))$. Similarly one obtains that sub-protocol P_2 fails with probability $p_{P_2} \in O(\exp(-\sqrt{n}))$ which implies that $p_f \in O(\exp(-\sqrt{n}))$, thereby proving $\varepsilon_{\mathrm{H}} \in O(\exp(-\sqrt{n}))$ as claimed. □

Observe that equation (G7) is restricted to i.i.d. initial states rather than arbitrary initial states and does not take into account Eve's purification of the initial states. But since theorem 1 of the main text is also applicable to the multiparty hashing protocol, we eliminate these issues and immediately infer for the multiparty hashing protocol prepended by symmetrization by using (G7) that

$$\|\mathcal{E}^s - \mathcal{F}^s\|_\diamond \leqslant 4(n + kn + 1)^{4^M - 1} \sqrt{\varepsilon_{\mathrm{H}}}. \tag{G15}$$

The proof of (G15) is simple: theorem 1 of the main text applies to the multiparty hashing protocol with $d = 2^M$, where M denotes the number of participants. Hence (G7) implies (G15) via theorem 1 of the main text.

ORCID iDs

A Pirker https://orcid.org/0000-0003-1260-1981

References

[1] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[2] Renner R 2005 *PhD Thesis* ETH Zurich
[3] Zhao Y-B and Yin Z-Q 2014 *Int. J. Mod. Phys. Conf. Ser.* **33** 1460370
[4] Gottesman D and Lo H-K 2003 *IEEE Trans. Inf. Theory* **49** 457
[5] Lo H-K 2001 *J. Phys. A: Math. Gen.* **34** 6957
[6] Gottesman D, Lo H-K, Lütkenhaus N and Preskill J 2004 *Quantum Inf. Comput.* **4** 325
[7] Lo H-K and Chau H F 1999 *Science* **283** 2050
[8] Acín A, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 *Phys. Rev. Lett.* **98** 230501
[9] Lim C C W, Portmann C, Tomamichel M, Renner R and Gisin N 2013 *Phys. Rev.* X **3** 031006
[10] Vazirani U and Vidick T 2014 *Phys. Rev. Lett.* **113** 140501
[11] Tomamichel M and Leverrier A 2017 *Quantum* **1** 14
[12] Biham E, Boyer M, Boykin P O, Mor T and Roychowdhury V 2006 *J. Cryptol.* **19** 381
[13] Mayers D 2001 *J. ACM* **48** 351
[14] Acin A, Cirac J I and Lewenstein M 2007 *Nat. Phys.* **3** 256
[15] Meter R V and Touch J 2013 *IEEE Commun. Mag.* **51** 8
[16] Kimble H J 2008 *Nature* **453** 1023
[17] Xu G-B, Wen Q-Y, Gao F and Qin S-J 2014 *Quantum Inf. Process.* **13** 2587
[18] Sun Z, Yu J and Wang P 2016 *Quantum Inf. Process.* **15** 373
[19] Sun Z, Zhang C, Wang P, Yu J, Zhang Y and Long D 2016 *Int. J. Theor. Phys.* **55** 1920
[20] Cirac J I, Ekert A K, Huelga S F and Macchiavello C 1999 *Phys. Rev.* A **59** 4249
[21] Portmann C 2017 Quantum authentication with key recycling *Advances in Cryptology* ed J-S Coron and J B Nielsen (Cham: Springer International Publishing) pp 339–68
[22] Garg S, Yuen H and Zhandry M 2017 New security notions and feasibility results for authentication of quantum data *Advances in Cryptology* ed J Katz and H Shacham (Cham: Springer International Publishing) pp 342–71
[23] Broadbent A and Wainewright E 2016 Efficient simulation for quantum message authentication *Information Theoretic Security* ed A C A Nascimento and P Barreto (Cham: Springer International Publishing) pp 72–91
[24] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wootters W K 1993 *Phys. Rev. Lett.* **70** 1895
[25] Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S and Sanpera A 1996 *Phys. Rev. Lett.* **77** 2818
[26] Bennett C H, Brassard G, Popescu S, Schumacher B, Smolin J A and Wootters W K 1996 *Phys. Rev. Lett.* **76** 722
[27] Aschauer H and Briegel H J 2002 *Phys. Rev. Lett.* **88** 047902
[28] Pirker A, Dunjko V, Dür W and Briegel H J 2017 *New J. Phys.* **19** 113012
[29] Bennett C H, DiVincenzo D P, Smolin J A and Wootters W K 1996 *Phys. Rev.* A **54** 3824

[30] Aschauer H, Dür W and Briegel H-J 2005 *Phys. Rev.* A **71** 012319
[31] Kruszynska C, Miyake A, Briegel H J and Dür W 2006 *Phys. Rev.* A **74** 052316
[32] Chen K and Lo H-K 2007 *Quantum Inf. Comput.* **7** 689
[33] Maneva E N and Smolin J A 2000 arXiv:quant-ph/0003099
[34] Hostens E, Dehaene J and De Moor B 2006 *Phys. Rev.* A **73** 042316
[35] Glancy S, Knill E and Vasconcelos H M 2006 *Phys. Rev.* A **74** 032319
[36] Hostens E, Dehaene J and De Moor B 2006 *Phys. Rev.* A **74** 062318
[37] Zwerger M, Pirker A, Dunjko V, Briegel H J and Dür W 2018 *Phys. Rev. Lett.* **120** 030503
[38] Schumacher B 1995 *Phys. Rev.* A **51** 2738
[39] Chor B, Goldreich O, Hastad J, Friedman J, Rudich S and Smolensky R 1985 The bit extraction problem or t-resilient functions *26th Annual Symposium on Foundations of Computer Science (sfcs 1985)* pp 396–407
[40] Zwerger M, Briegel H J and Dür W 2014 *Phys. Rev.* A **90** 012314
[41] Raussendorf R, Browne D E and Briegel H J 2003 *Phys. Rev.* A **68** 022312
[42] Zwerger M, Briegel H J and Dür W 2013 *Phys. Rev. Lett.* **110** 260503
[43] Pirker A, Wallnöfer J and Dür W 2018 *New J. Phys.* **20** 053054
[44] Horodecki K, Horodecki M, Horodecki P and Oppenheim J 2005 *Phys. Rev. Lett.* **94** 160502
[45] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2017 *Nat. Commun.* **8** 15043
[46] Christandl M, König R and Renner R 2009 *Phys. Rev. Lett.* **102** 020504
[47] Wallnöfer J and Dür W 2017 *Phys. Rev.* A **95** 012303
[48] Kitaev A Y 1997 *Russ. Math. Surv.* **52** 1191
[49] Aschauer H and Briegel H J 2002 *Phys. Rev.* A **66** 032302
[50] Dür W, Briegel H-J, Cirac J I and Zoller P 1999 *Phys. Rev.* A **59** 169
[51] Bennett C H, Brassard G, Crépeau C and Maurer U 1995 *IEEE Trans. Inf. Theory* **41** 1915
[52] Raussendorf R and Briegel H J 2001 *Phys. Rev. Lett.* **86** 5188
[53] Briegel H J, Browne D E, Dür W, Raussendorf R and Van den Nest M 2009 *Nat. Phys.* **5** 19
[54] Briegel H J and Raussendorf R 2001 *Phys. Rev. Lett.* **86** 910
[55] Zwerger M, Dür W and Briegel H J 2012 *Phys. Rev.* A **85** 062326
[56] Dür W, Hein M, Cirac J I and Briegel H-J 2005 *Phys. Rev.* A **72** 052326
[57] Zwerger M, Briegel H J and Dür W 2016 *Appl. Phys.* B **122** 1
[58] Bennett G 1962 *J. Am. Stat. Assoc.* **57** 33
[59] Love E R 1980 *Math. Gazette* **64** 55
[60] Hoeffding W 1963 *J. Am. Stat. Assoc.* **58** 13