Cost of quantum secret key

Karol Horodecki,* Siddhartha Das,† Leonard Sikorski,‡ and Mark M. Wilde§

Background.—Quantum mechanics is a rather surprising physical theory, as it is reversible in principle, contrary to our common experience. After an arbitrary quantum operation is applied to a system, if full access to its environment is available, the system's state can be set back to its initial form by an inverse operation. However, in practice, reversibility is usually not possible. The system, after an operation, typically becomes entangled with an inaccessible environment in an irreversible way. This irreversibility can be quantified in different ways in the resource-theoretic framework [1], which was first introduced and studied for the case of the resource theory of entanglement [2].

The origin of irreversibility is even more fundamental in the case of the resource of quantum secret key. In this setting, an eavesdropper or hacker will never give back a system that has leaked, even if it might be possible in practice. This fact was first noticed and studied in the classical scenario of secret key agreement (SKA) [3, 4]. There, the adversary has only a classical memory Z and eavesdrops on two honest parties, who possess classical random variables X and Y, respectively, and transform them by local (classical) operations and public communication. Inspired by an apparent correspondence between entanglement theory and SKA established in [5], it was proved that the cost of creating a distribution sometimes exceeds its distillable secure content in the SKA scenario [4] (see also [6–10] for related work). Key distillation for the quantum generalization of SKA has been studied in [11–13] via a mapping of tripartite distributions into pure tripartite states, as proposed in [14].

Building a quantum internet infrastructure is one of the main visions of the quantum information community [15]. It is then important to understand the cost of the network's constituents, i.e., quantum states and channels with secure key. Indeed, since pure entanglement is not a precondition of quantum security [16, 17], we assert here that secure key is the proper resource for quantifying the information-theoretic expense of the quantum-secured internet.

While entanglement theory has been thoroughly studied [18] since its invention [2, 19], the resource theory of private key secure against a quantum adversary has yet to be developed fully from the resource-theoretic perspective. On the one hand, lower and upper bounds on the distillable key have been developed thoroughly, starting from the seminal protocols BB84 and E91 [20, 21] and their followups [22–27] in a number of cryptographic scenarios (cf. [28, 29]). Also, the distillable key K_D has been shown to be an entanglement measure and studied in [16, 17, 30]. On the other hand, to our knowledge, the privacy cost has hitherto not been introduced nor studied in the fully quantum setup. It is important to note that the resource theory of secure key differs from the resource theory of entanglement. This is because there exist states that contain no distillable entanglement ($E_D = 0$) [31], but contain a strictly positive rate of distillable key K_D secure against a quantum adversary [16, 17].

Objectives.—Motivated by this, we initiate the study of the cost of secret key and understanding the problem of irreversibility in the quantum cryptographic scenario Indeed, it is natural

* Institute of Informatics, National Quantum Information Centre, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, Wita Stwosza 57, 80-308 Gdańsk, Poland; International Centre for Theory of Quantum Technologies, University of Gdańsk, Wita Stwosza 63, 80-308 Gdańsk, Poland; School of Electrical and Computer Engineering, Cornell University, Ithaca, New York 14850, USA

† Center for Security, Theory and Algorithmic Research, Centre of Quantum Science and Technology, International Institute of Information Technology, Hyderabad, Gachibowli, Telangana 500032, India

‡ Faculty of Mathematics Physics and Informatics, University of Gdańsk, Wita Stwosza 57, 80-308 Gdańsk, Poland

§ School of Electrical and Computer Engineering, Cornell University, Ithaca, New York 14850, USA

to postulate that the strict gap between the key cost and distillable key in quantum networks is a natural quantifier of the lower bound on the inevitable energy cost of operating the quantum network. This cost may eventually become a non-negligible part of the energy spent on running quantum network, if a sufficiently large amount of data is transmitted.

In the most basic case of a point-to-point connection in the network, the two honest parties share a bipartite quantum state and process it by LOCC. Assuming the worst case, the quantum eavesdropper has access to a purifying system of a purification [32] of the state of the honest parties and obtains any classical communication and any system traced out by them during LOCC processing. The main question we pose in this setting is as follows:

- "How much private key is needed for the creation of an arbitrarily good approximation of n copies of a bipartite quantum state by LOCC, for sufficiently large n?"

With this in mind, we depart from the above approach of exploring the embedding of SKA into the quantum scenario [1]. Instead, we develop the resource theory of key secure against a quantum adversary. We do so according to the current state of the art, under assumption that there are no entangled states with zero distillable key (see the 24th open problem on the IQOQI Vienna list [33]).

Main results.—We define and characterize the key cost K_C, a fundamental quantity in the resource theory of privacy. The key cost is an upper bound on the distillable key secure against a quantum eavesdropper, and it indicates how much key one needs to invest when creating a quantum state. In order to characterize the key cost, we introduce and study another quantity, the key of formation K_F. Informally, K_F is equal to the minimum average amount of key content of a state, where the average is taken over all decompositions of the state into a finite mixture of pure states that are Schmidt-twisted [34, 35], which we refer to as generalized private states. A generalized private state $\gamma(\psi)$ has the structure of a private state with a pure bipartite state ψ "twisted" (i.e. rotated by a control unitary transformation) instead of the maximally entangled state Φ^+. Also the controlled unitary which performs the "twisting" has its control basis set to be the Schmidt basis of ψ. One of our main results, relating the key cost and the key of formation, is encapsulated in the following equation:

$$K_C(\rho) = K_F^{\infty}(\rho), \tag{1}$$

where $K_F^{\infty} := \lim_{n\to\infty} \frac{1}{n} K_F(\rho^{\otimes n})$.

We note here that key cost and key of formation are analogous to the entanglement cost E_C and entanglement of formation E_F in entanglement theory [2], respectively. Furthermore, the aforementioned generalized private states form a class of states in the privacy domain that corresponds to the class of pure states in entanglement theory. Also, the equality in (1) is analogous to the relation $E_F^{\infty}(\rho) = E_C(\rho)$ from entanglement theory [36]. Although there are analogies between entanglement and private key [5, 14], we should note that there are important distinctions, some of which have led to profound insights into the nature of quantum information [37–39]. Additionally, the technicalities of dealing with privacy are more subtle and involved than when dealing with entanglement [16, 17]. For our specific problem considered here, i.e., to obtain (1), it was necessary for us to develop techniques beyond what is currently known in entanglement theory. Indeed, our main technical contribution here, for establishing (1), involves designing a protocol that dilutes privacy.

[1] We consider, in fact, processing of an arbitrary pure state $|\psi\rangle_{ABE}$ (such that $\mathrm{Tr}_E|\psi\rangle\langle\psi|_{ABE} = \rho$) by (quantum) local operations and public communication. The pure state $|\psi\rangle_{ABE}$ in our approach may not originate from any classical distribution via the Collins–Popescu mapping.

As additional results, we prove the asymptotic continuity and monotonicity of K_F; as a consequence, it follows that $K_F^\infty(\rho) \coloneqq \lim_{n\to\infty} \frac{1}{n} K_F(\rho^{\otimes n}) \leq K_C(\rho)$ holds for every bipartite state ρ. A strengthening of this inequality occurs for strictly irreducible generalized private states: we have that $K_F(\rho) = \inf_{\{(p_k,\gamma(\psi_k))\}} \sum_k p_k K_D(\gamma(\psi_k))$. Combining these observations with other bounds, we conclude that

$$K_D(\gamma(\psi)) = K_F(\gamma(\psi)) = E_R(\gamma(\psi)) = E_R^\infty(\gamma(\psi)) = K_C(\gamma(\psi)) = S_A(\psi) = S_{A_K}(\gamma(\psi)), \tag{2}$$

where $S_A(\rho)$ denotes the von Neumann entropy of the reduced state of ρ on system A. We note that these equalities are appealing, in analogy with what happens for pure states ψ in entanglement theory, for which the distillable entanglement, relative entropy of entanglement, and entanglement cost all coincide and are equal to the von Neumann entropy of the marginal of ψ. The difference in this context is that system A_K is only the "key part" subsystem of $\gamma(\psi)$, and not the full local subsystem.

The core of the characterization of K_C via Eq. (1) is a dilution protocol (DP). It allows for establishing the inequality opposite to the one shown above, i.e., $K_F^\infty(\rho) \geq K_C(\rho)$. This protocol transforms a private state via LOCC into an approximation of a large number of copies of the desired generalized private state. Our idea diverges from the one of [40], where dilution of entanglement has been proposed using pure entanglement, and quantum teleportation [2] because the private states have, in general, a low amount of pure entanglement. While most of the aforementioned results hold for the asymptotic definition of the key cost, we also prove a yield-cost relation in the one-shot scenario that bounds the one-shot distillable key from above by the one-shot key cost and a small correction factor.

Applications.—The applicability of the introduced quantities goes beyond the resource theory of (device-dependent) private key. We see that K_F and K_C are novel entanglement measures. They also naturally fit the scenario in which security is independent of the inner workings of the devices (device-independent security [41]). Indeed, by the technique of [42], the *reduced* versions of K_C and K_F are novel measures of Bell non-locality [43]. More importantly, the single-shot version of the reduced K_C, that is, the reduced single-shot key cost $K_C^{\varepsilon\downarrow}$, can be treated as definition of the key cost of a device — a quantity that has not been considered so far. The new entanglement measures can also be lifted to the dynamic scenario of quantum channels, in which the privacy cost of a quantum channel can be defined. This cost can be further expressed as the key cost of the Choi state of the channel if the latter has sufficient symmetry.

Summary.—In this work, we develop the resource theory of quantum secret key. Operating under the assumption that entangled states with zero distillable key *do not* exist, we define the *key cost* of a quantum state, channel, and device. We study its properties through the lens of a quantity that we call the *key of formation*. The main result of our work is that the regularized key of formation equals the key cost of a quantum state. The core protocol underlying this result is privacy dilution, which converts states containing ideal privacy into ones with diluted privacy. Additionally, our main result follows by proving that the key of formation is an entanglement monotone with appealing mathematical properties. We further focus on mixed-state analogues of pure quantum states in the domain of privacy, and we prove that a number of entanglement measures are equal to each other for these states, similar to the case of pure entangled states. The privacy cost in the single-shot regime exhibits a yield-cost relation, and basic results for quantum channels and devices are also provided.

[1] E. Chitambar and G. Gour, Quantum resource theories, Reviews of Modern Physics **91**, 025001 (2019).

[2] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Purification of noisy entanglement and faithful teleportation via noisy channels, Physical Review Letters **76**, 722 (1996), quant-ph/9511027.

[3] U. M. Maurer, Secret key agreement by public discussion from common information, IEEE Transactions on Information Theory **39**, 733 (1993).

[4] R. Renner and S. Wolf, New bounds in secret-key agreement: The gap between formation and secrecy extraction, in *Lecture Notes in Computer Science* (Springer Berlin Heidelberg, 2003) pp. 562–577.

[5] N. Gisin and S. Wolf, Linking classical and quantum key agreement: Is there "bound information"?, in *Proceedings of Crypto 2000, Lecture Notes in Computer Science*, Vol. 1880 (2000) pp. 482–500.

[6] A. Acín, J. I. Cirac, and L. Masanes, Multipartite bound information exists and can be activated, Physical Review Letters **92**, 107903 (2004).

[7] A. Winter, Secret, public and quantum correlation cost of triples of random variables, in *Proceedings of the 2005 International Symposium on Information Theory* (2005) pp. 2270–2274.

[8] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Information theories with adversaries, intrinsic information, and entanglement, Foundations of Physics **35**, 2027 (2005).

[9] E. Chitambar, M.-H. Hsieh, and A. Winter, The private and public correlation cost of three random variables with collaboration, IEEE Transactions on Information Theory **62**, 2034 (2016).

[10] E. Chitambar, B. Fortescue, and M.-H. Hsieh, Classical analog to entanglement reversibility, Physical Review Letters **115**, 090501 (2015).

[11] M. Christandl, A. Ekert, M. Horodecki, P. Horodecki, J. Oppenheim, and R. Renner, Unifying classical and quantum key distillation, in *Theory of Cryptography* (Springer Berlin Heidelberg, 2007) pp. 456–478.

[12] M. Ozols, G. Smith, and J. A. Smolin, Bound entangled states with a private key and their classical counterpart, Physical Review Letters **112**, 110502 (2014).

[13] E. Chitambar, B. Fortescue, and M.-H. Hsieh, The conditional common information in classical and quantum secret key distillation, IEEE Transactions on Information Theory **64**, 7381 (2018).

[14] D. Collins and S. Popescu, Classical analog of entanglement, Physical Review A **65**, 032321 (2002).

[15] S. Wehner, D. Elkouss, and R. Hanson, Quantum internet: A vision for the road ahead, Science **362**, 10.1126/science.aam9288 (2018), https://science.sciencemag.org/content/362/6412/eaam9288.full.pdf.

[16] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Secure key from bound entanglement, Physical Review Letters **94**, 160502 (2005).

[17] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, General paradigm for distilling classical key from quantum states, IEEE Transactions on Information Theory **55**, 1898 (2009).

[18] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Reviews of

Modern Physics **81**, 865 (2009).

[19] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Mixed-state entanglement and quantum error correction, Physical Review A **54**, 3824 (1996), quant-ph/9604024.

[20] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (India, 1984) p. 175.

[21] A. K. Ekert, Quantum cryptography based on bell's theorem, Physical Review Letters **67**, 661 (1991).

[22] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Reviews of Modern Physics **74**, 145 (2002).

[23] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **461**, 207 (2005).

[24] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-independent security of quantum cryptography against collective attacks, Physical Review Letters **98**, 230501 (2007).

[25] M. Pawłowski and N. Brunner, Semi-device-independent security of one-way quantum key distribution, Physical Review A **84**, 010302 (2011).

[26] H.-K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, Physical Review Letters **108**, 130503 (2012).

[27] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, Practical device-independent quantum cryptography via entropy accumulation, Nature Communications **9**, 459 (2018).

[28] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Reviews of Modern Physics **92**, 025002 (2020).

[29] S. Das, S. Bäuml, M. Winczewski, and K. Horodecki, Universal limitations on quantum key distribution over a network, Physical Review X **11**, 041016 (2021).

[30] M. Christandl, *The Structure of Bipartite Quantum States - Insights from Group Theory and Cryptography*, Ph.D. thesis, - (2006).

[31] M. Horodecki, P. Horodecki, and R. Horodecki, Mixed-state entanglement and distillation: Is there a "bound" entanglement in nature?, Physical Review Letters **80**, 5239 (1998).

[32] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press,Cambridge, 2000).

[33] Open quantum problems—IQOQI Vienna, https://oqp.iqoqi.oeaw.ac.at/open-quantum-problems.

[34] K. Horodecki, M. Studziński, R. P. Kostecki, O. Sakarya, and D. Yang, Upper bounds on the leakage of private data and an operational approach to Markovianity, Physical Review A **104**, 052422 (2021).

[35] K. Horodecki, *General paradigm for distilling classical key from quantum states — On quantum entanglement and security*, Ph.D. thesis, University of Warsaw (2008).

[36] P. M. Hayden, M. Horodecki, and B. M. Terhal, The asymptotic entanglement cost of preparing a

quantum state, Journal of Physics A: Mathematical and General **34**, 6891 (2001).

[37] K. Horodecki, M. Horodecki, P. Horodecki, D. Leung, and J. Oppenheim, Unconditional privacy over channels which cannot convey quantum information, Physical Review Letters **100**, 110502 (2008).

[38] K. Horodecki, M. Horodecki, P. Horodecki, D. Leung, and J. Oppenheim, Quantum key distribution based on private states: Unconditional security over untrusted channels with zero quantum capacity, IEEE Transactions on Information Theory **54**, 2604 (2008).

[39] G. Smith and J. Yard, Quantum communication with zero-capacity channels, Science **321**, 1812 (2008), 0807.4935.

[40] H.-K. Lo and S. Popescu, Classical communication cost of entanglement manipulation: Is entanglement an interconvertible resource?, Physical Review Letters **83**, 1459 (1999).

[41] I. W. Primaatmaja, K. T. Goh, E. Y. Z. Tan, J. T. F. Khoo, S. Ghorai, and C. C. W. Lim, Security of device-independent quantum key distribution protocols: a review, (2022), arXiv:2206.04960.

[42] M. Christandl, R. Ferrara, and K. Horodecki, Upper bounds on device-independent quantum key distribution, Physical Review Letters **126**, 160501 (2021).

[43] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Reviews of Modern Physics **86**, 419 (2014).