Fully device independent Conference Key Agreement

(see arXiv:1708.00798)

Jérémy Ribeiro, Gláucia Murta, and Stephanie Wehner

QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands

Quantum communication allows cryptographic security that is provably impossible to obtain using any classical means. Probably the most famous example of a quantum advantage is quantum key distribution (QKD) [1, 2], which allows two parties Alice and Bob to exchange an encryption key whose security is guaranteed even if the adversary has an arbitrarily powerful quantum computer. What's more, properties of entanglement lead to the remarkable feature that security is sometimes possible even if the quantum devices used to execute the protocol are largely untrusted. Specifically, the notion of *device independent (DI)* security [3, 4] models quantum devices as black boxes in which we may only choose measurement settings and observe measurement outcomes. Yet, the quantum state and measurements employed by such boxes are unknown, and may even be prepared arbitrarily by the adversary.

Significant efforts have been undertaken to establish the security of device independent QKD [4–10], leading to ever more sophisticated security proofs (see e.g. [7–10]). Initial proofs assumed a simple model in which the devices act independently and identically (i.i.d.) in each round. This assumption significantly simplifies the analysis, since the underlying properties of the devices may first be estimated by gaining statistical confidence from the observations of measurement outcomes. The main challenge overcome by the more recent security proofs was to establish security, even if the devices behave arbitrarily from one round to the next, including having an arbtirary memory of the past that they might use to thwart the efforts of Alice and Bob. Assuming that the devices carry at least some memory of past interactions is an extremely realistic assumption due to technical limitations, even if Alice and Bob prepare their own trusted, but imperfect, devices, highlighting the extreme importance of such analyses for the implementation of device independent QKD. In contrast, relatively little is known about device independence outside the realm of QKD [11–14].

Conference key agreement [15, 16] (CKA or N-CKA) is the task of distributing a secret key among N parties. In order to achieve this goal, one could make use of $N-1$ individual QKD protocols to distribute $N-1$ different keys between one of the parties (Alice) and the others ($\mathrm{Bob}_1, \ldots, \mathrm{Bob}_{N-1}$), followed by Alice using these keys to encrypt a common key to all the participants. However the existence of genuine multipartite quantum correlations can bring some advantage to multipartite tasks, and, as shown in Ref. [16], exploring properties of genuine multipartite entanglement can lead to protocols with better performance for conference key agreement.

I. RESULTS

Here we present the first ever security analysis of Conference Key Agreement (CKA) in the most paranoid model of device independence. Our protocol can be implemented using hardware that is capable of performing Bell tests (specifically, the Mermin-Ardehali-Belinskii-Klyshko (MABK) [17–19] inequality), and security can in principle be obtained for any violation of the MABK inequality that detects genuine multipartite entanglement among the N parties involved in the protocol.

Instead of relying on EPR pairs, our protocol uses an N-partite GHZ state and employs the MABK inequality to perform a Bell test to gain device independence. Note that one could of course use $N-1$ QKD protocols to distribute $N-1$ different keys between one of the parties (Alice) and the others (Bob_1,...,Bob_{N-1}), and then Alice would use these keys to one time pad one common key to all the Bobs. However, we show that if we apply the same type of noise on each qubit, then the N-CKA protocol does in fact produce a shared key at a higher rate than using pairwise device

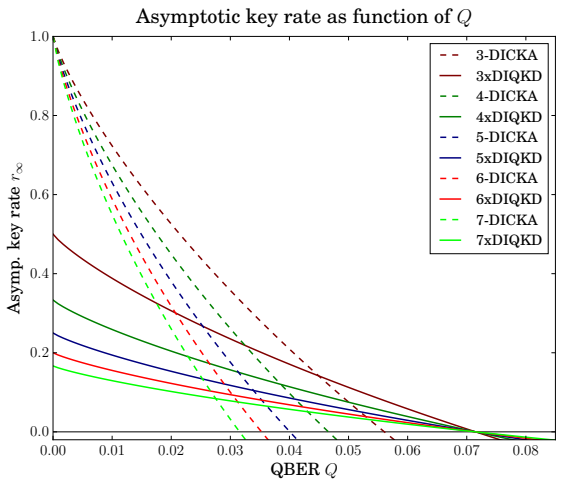

Figure 1. Asymptotic key rate for N-device independent CKA (N-DICKA, dashed lines), and for the distribution of a secret key between N parties through $N-1$ device independent quantum key distribution ($(N-1)\times$DIQKD) protocols (solid lines), when each qubit experiences independent bit errors measured at a bit error rate (QBER) Q. From top to bottom, the lines correspond to $N = \{3, 4, 5, 6, 7\}$. We observe that for low noise it is advantageous to use our DICKA protocol instead of using $N-1$ DIQKD protocols [10]. In general, the comparison between the two methods depends on the cost and noisiness of producing GHZ states over pairwise EPR pairs.

independent QKD for low noise (see Fig. 1).

II. METHODS

- To establish security, we make use of a recently developed tool, the Entropy Accumulation Theorem (EAT) [20], which decomposes the (conditional) smooth min-entropy of n subsystems (evaluated on a state conditioned on observing some event, like the violation of a Bell inequality) into the sum of the (conditional) Von Neumann entropy of each subsystem.

- In addition to EAT, we need to generalize a bound (function of the CHSH violation the state attains) on the Holevo information derived in [5, Section 2.3] to the N-partite case. To do so, we studied a suitable family of inequalities, Mermin-Ardehali-Belinskii-Klyshko (MABK) inequalities [17–19], between N parties. As a conceptually appealing observation, we prove our result by reinterpreting the MABK inequalities as a CHSH inequality between one of the parties, and all the other parties together.

- The error correction and parameter estimation protocols also have to be adapted to the case of N parties. Similarly to [10] we perform parameter estimation together with error correction. However, in the N-partite scenario each Bob has to send an additional amount of error correcting information for the estimation of the Bell violation requiring analysis.

[1] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67:661–663, 1991.
[2] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560, Part 1:7 – 11, 2014. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of {BB84}.
[3] D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, FOCS '98, pages 503–, Washington, DC, USA, 1998. IEEE Computer Society.
[4] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 98:230501, 2007.
[5] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4):045021, 2009.

[6] L. Masanes, S. Pironio, and A. Acín. Secure device-independent quantum key distribution with causally independent measurement devices. *Nature Communications*, 2011.

[7] C. A. Miller and Y. Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. *arXiv:1402.0489*, 2014.

[8] C. A. Miller and Y. Shi. Universal security for randomness expansion from the spot-checking protocol. *arXiv:1411.6608*, 2014.

[9] U. Vazirani and T. Vidick. Fully device-independent quantum key distribution. *Phys. Rev. Lett.*, 113:140501, 2014.

[10] R. Arnon-Friedman, R. Renner, and T. Vidick. Simple and tight device-independent security proofs. *arXiv:1607.01797*, 2016.

[11] J. Ribeiro, L. Phuc Thinh, J. Kaniewski, J. Helsen, and S. Wehner. Device-independence for two-party cryptography and position verification. *arXiv:1606.08750*, 2016.

[12] J. Silman, A. Chailloux, N. Aharon, I. Kerenidis, S. Pironio, and S. Massar. Fully distrustful quantum bit commitment and coin flipping. *Phys. Rev. Lett.*, 106:220501, 2011.

[13] A. Kent. Quantum tagging for tags containing secret classical data. *Phys. Rev. A*, 84:022335, 2011.

[14] M. Tomamichel, S. Fehr, J. Kaniewski, and S. Wehner. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New Journal of Physics*, 2013.

[15] K. Chen and H.-K. Lo. Conference key agreement and quantum sharing of classical secrets with noisy GHZ states. In *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005.*, pages 1607–1611, 2005.

[16] M. Epping, H. Kampermann, C. Macchiavello, and D. Bruß. Multi-partite entanglement speeds up quantum key distribution in networks. *arXiv:1612.05585*, 2016.

[17] N. D. Mermin. Extreme quantum entanglement in a superposition of macroscopically distinct states. *Phys. Rev. Lett.*, 65:1838–1840, 1990.

[18] M. Ardehali. Bell inequalities with a magnitude of violation that grows exponentially with the number of particles. *Phys. Rev. A*, 46:5375–5378, 1992.

[19] A. V. Belinskiĭ and D. N. Klyshko. Interference of light and Bell's theorem. *Physics-Uspekhi*, 36(8):653, 1993.

[20] F. Dupuis, O. Fawzi, and R. Renner. Entropy accumulation. *arXiv:1607.01796*, 2016.