Composable Security of Measurement-Device-Independent Continuous-Variable Quantum Key Distribution against Coherent Attacks

Cosmo Lupo, Carlo Ottaviani, Panagiotis Papanastasiou, Stefano Pirandola
York Centre for Quantum Technologies (YCQT), University of York, York YO10 5GH, UK

Introduction. Quantum communication technologies, particularly quantum key-distribution (QKD), progress rapidly from research laboratories towards real-world implementations. The ultimate goal is building a network of quantum devices (quantum internet) enabling unconditionally secure communications on the global scale [1–4]. To this end, QKD has been recently extended to a scenario where two honest users (Alice and Bob) exploit the mediation of a (possibly untrusted) relay, operated by the eavesdropper (Eve), to establish a secure communication channel [5, 6]. This remarkable feature is made possible by the working mechanism of the relay itself, which activates secret correlations on the parties' remote stations by performing Bell detection on the incoming signals and publicly announcing the results [6]. This architecture has been called measurement-device independent (MDI) QKD because, as such, the privacy of the communication does not rely on the trustability of the parties' detection devices [5, 6]. These are in fact more exposed to side-channel attacks than other devices controlled by the parties. In addition to this, MDI-QKD allows to distribute secret key preserving a basic network structure.

Recently, protocols exploiting quantum continuous variables (CV) attracted considerable attention, for their potential of boosting the communication rate, and for their employability in mid-range (metropolitan), high-rate quantum cryptography [6, 7]. In particular CV protocols based on Gaussian operations [8] have been deeply studied for their relatively simple implementation. The security of Gaussian protocols is today very well established assuming ideal conditions: Alice and Bob exchanging an asymptotically large number of signals. By contrast, in realistic conditions the parties can extract a secret-key only from a finite number of signals. For this reason, the security analysis of CV protocols progressed towards the incorporation of finite-size effects within a composable framework [9–13].

In this landscape, a composable security proof for CV MDI-QKD is still missing. Given the considerable interest in this layout, and its importance in the implementation of future quantum networks, this work fills this gap by providing a rigorous composable-security proof of CV MDI-QKD. We first prove the security against collective Gaussian attacks by applying a new bound on the conditional smooth min-entropy (see [14] for details). Then, using recent results [10], we extend our proof to the most general class of coherent attacks.

Outline of the protocol. In the entanglement-based representation, Alice and Bob locally prepare a pair of two-mode squeezed vacuum states. They retain one mode and send the other one to Eve. Eve jointly measures the incoming signals by applying continuous-variable Bell detection. The outcomes of such a measurement is broadcast to Alice and Bob. Finally, both Alice and Bob measure their local modes by heterodyne detection, obtaining the classical variables X and Y. Equivalently, in the prepare-and-measure representation (shown in Fig. 1), Alice and Bob independently prepare coherent states according to a Gaussian distribution.

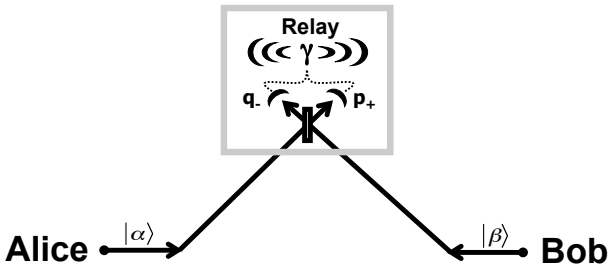

FIG. 1: In a prepare-and-measure CV MDI QKD protocol, Alice and Bob send coherent states $|\alpha\rangle$, $|\beta\rangle$ (corresponding to the variables X and Y respectively) to the relay. The relay applies a Bell measurement to the incoming signals, and broadcast the result γ (corresponding to the variable Z) to Alice and Bob.

Since the parties perform local heterodyne detection the cardinality of X and Y is in principle infinite. However, in practice one can always apply an Analog to Digital Conversion (ADC) algorithm in order to make the variables X and Y discrete and bounded. We therefore assume that X and Y are discrete variables with cardinality 2^{2d} (i.e., d bits per quadrature).

Security analysis. According to the leftover hash lemma, the number of (approximately) secret bits that can be extracted from the raw key is lower bounded by the conditional smooth min-entropy of X (we assume reconciliation on Alice's), conditioned on the quantum state of the eavesdropper (which in our setting includes both the quantum part E^n and the classical part Z^n) [15]

$$s_n^{\epsilon+\epsilon_{\rm EC}} \geq H_{\min}^{\epsilon}(X^n|E^nZ^n)_{\rho^n} - {\rm leak}_{\rm EC}(n,\epsilon_{\rm EC})\,, \qquad (1)$$

where we have also subtracted the information leakage ${\rm leak}_{\rm EC}(n,\epsilon_{\rm EC})$ necessary for EC. The security parameter $\epsilon+\epsilon_{\rm EC}$ comprises of two terms: ϵ is the smoothing parameter entering the smooth conditional min-entropy, and $\epsilon_{\rm EC}$ is the error in the EC routine.

To proceed with the security analysis, we first assume that Eve operates a collective Gaussian attack. For collective attacks, the state ρ^n shared by Alice, Bob, and Eve, can be taken to have a tensor-power structure, i.e., $\rho^n=\rho^{\otimes n}$. On the other hand, the state that is actually used for key generation is the

one conditioned upon EC and PE being successful. Because EC and PE have a non-zero failure probability, the conditional state is no longer guaranteed to be a tensor-power. Indeed, the conditioned state have the form $\rho^n = p^{-1}\Pi\rho^{\otimes n}\Pi$, where Π is a projector operator (projecting on the subspace in which EC and PE do not abort), and $p = \mathrm{Tr}(\Pi\rho^{\otimes n}\Pi)$ is the probability of successful EC and PE [9]. Notwithstanding, we are able to show (details are provided in [14]) that the state can still be assumed to be a tensor-power upon replacing $\epsilon \to \frac{2}{3}p\epsilon$ and shortening the secret key by a small amount of $\log\left(p - \frac{2}{3}p\epsilon\right)$ bits, that is,

$$s_n^{\epsilon+\epsilon_{\mathrm{EC}}} \geq H_{\min}^{\frac{2}{3}p\epsilon}(X^n|E^nZ^n)_{\rho^{\otimes n}} - \mathrm{leak}_{\mathrm{EC}}(n,\epsilon_{\mathrm{EC}}) + \log\left(p - \frac{2}{3}p\epsilon\right). \quad (2)$$

The conditional smooth min-entropy can be estimated using the Asymptotic Equipartition Property (AEP), which yields a bound in terms of the von Neumann conditional entropy [15]:

$$H_{\min}^{\delta}(X^n|E^nZ^n)_{\rho^{\otimes n}} \geq nH(X|EZ)_{\rho} - \sqrt{n}\,\Delta_{\mathrm{AEP}}(\delta,d)\,,$$

where

$$\Delta_{\mathrm{AEP}}(\delta,d) \simeq 4d\sqrt{\log\left(2/\delta^2\right)} \quad (3)$$

is also a function of the dimensionality parameter d. Applying the AEP to Eq. (2) we then obtain

$$s_n^{\epsilon+\epsilon_{\mathrm{EC}}} \geq nH(X|EZ)_{\rho} - \mathrm{leak}_{\mathrm{EC}}(n,\epsilon_{\mathrm{EC}}) - \sqrt{n}\,\Delta_{\mathrm{AEP}}\left(\frac{2}{3}p\epsilon,d\right) + \log\left(p - \frac{2}{3}p\epsilon\right). \quad (4)$$

The final step is to estimate the conditional entropy $H(X|EZ)$ by PE. Under the assumption of collective Gaussian attacks, it is sufficient to consider a realistic beam-splitter attack (possibly introducing excess noise) on the communication lines between the users and the relay [6]. In such a case the attenuation and excess noise can be evaluated from Alice and Bob joint covariance matrix.

Indeed, as recently shown in [10], the most general coherent attacks can be reduced to collective Gaussian attacks by applying a Gaussian de Finetti reduction, provided the protocol is symmetric under the linear passive unitary transformations (i.e., those transformations that can be generated by a network of beam splitters and phase shifters) locally applied by Alice and Bob. Since our protocol has the required symmetry, security against coherent attacks can be obtained by applying an energy test on a random subset of k modes. The resulting key has a security parameter replaced by $\epsilon \to \frac{K^4}{50}\epsilon$, with $K \sim n^4$, and it is shortened by $2\log\binom{K+4}{4}$ bits. We therefore obtain the following expression for the secret key length:

$$s_n^{\epsilon'} \geq n'\hat{H}(X|EZ) - \mathrm{leak}_{\mathrm{EC}}(n',\epsilon_{\mathrm{EC}}) - \sqrt{n'}\,\Delta_{\mathrm{AEP}}\left(\frac{2}{3}p\epsilon,d\right) + \log\left(p - \frac{2}{3}p\epsilon\right) - 2\log\binom{K+4}{4}, \quad (5)$$

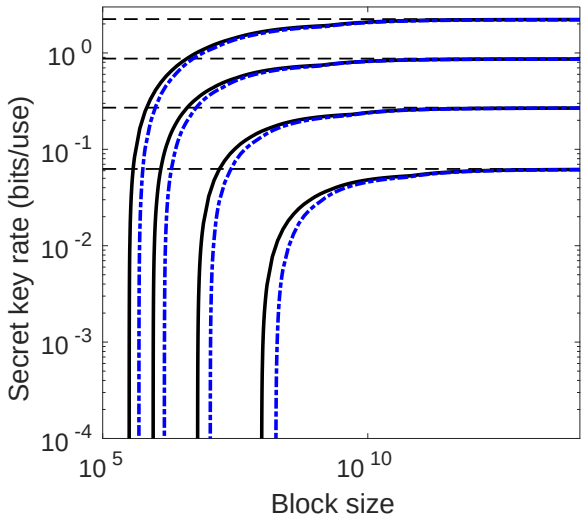

FIG. 2: Finite-size secret key rate (bits per signal) vs block size for Alice and Bob being located at the same distance from the relay (same value of the attenuation factors $\eta_A = \eta_B$). Solid black lines: collective Gaussian attacks. Dot-dashed blue lines: coherent attacks. Dashed black lines: asymptotic rates. From top to bottom, $\eta_A = \eta_B = 0.1dB, 0.3dB, 0.5dB, 0.6dB$. EC efficiency is $\beta = 0.95$, success probability $p = 0.99$, and the security parameter $\epsilon = 10^{-21}$.

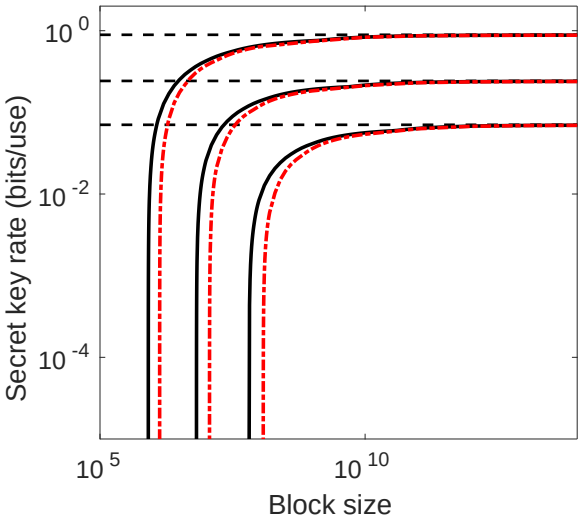

FIG. 3: Finite-size secret key rate (bits per signal) vs block size for Bob being located close to the relay (attenuation factor of the communication from Bob to the relay is $\eta_B = 0.99$). Solid black lines: collective Gaussian attacks. Dot-dashed red lines: coherent attacks. Dashed black lines: asymptotic rates. From top to bottom, signals from Alice to the relay are attenuated by $\eta_A = 1dB, 3dB, 5dB$. EC efficiency is $\beta = 0.95$, success probability $p = 0.99$, and the security parameter $\epsilon = 10^{-21}$.

where $\epsilon' = K^4(\epsilon+\epsilon_{\rm EC}+\epsilon_{\rm PE})/50$, and $\hat{H}(X|EZ)$ is a worst-case estimation for the conditional entropy that holds with an error smaller than $\epsilon_{\rm PE}$. Here $n' = n-k-m$ is the number of signal actually used for key extraction, where k signals are used for the energy test and m for PE. Figures 2, 3 show the rate $r_n = s_n/n$ vs the block size n in the symmetric and asymmetric configurations (see captions for details).

Conclusion. In this work we present for the first time a composable security proof for CV MDI QKD. As shown in Figures 2, 3, our results demonstrate that it is possible to achieve a nonzero secret key rate against the most general class of coherent attacks for block size of the order of $10^6 - 10^9$. Therefore, our results show that a field demonstration of CV MDI QKD is feasible with currently available technologies.

[1] H. J. Kimble, Nature **453**, 1023 (2008).

[2] S. Pirandola and S. L. Braunstein, Nature **532**, 169 (2016).

[3] S. Pirandola *et al.*, Nature Photon. **9**, 641 (2015).

[4] U. L. Andersen, J. S. Neergaard-Nielsen, P. van Loock, A. Furusawa, Nature Phys. **11**, 713 (2015).

[5] S. L. Braunstein, S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012); H.-K. Lo, M. Curty, B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[6] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, U. L. Andersen, Nature Photon. **9**, 397 (2015).

[7] S. Pirandola, C. Ottaviani, C. S. Jacobsen, G. Spedalieri, S. L. Braunstein, S. Lloyd, T. Gehring, U. L. Andersen, Nature Photon. **9**, 776 (2015).

[8] C. Weedbrook, S.Pirandola, R. García-Patrón, N. J. Cerf, T.C. Ralph, J. H. Shapiro, S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).

[9] A. Leverrier, Phys. Rev. Lett. **114**, 070501 (2015).

[10] A. Leverrier, arXiv: 1701.03393 (2017).

[11] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, R. F. Werner, Phys. Rev. Lett. **109**, 100502 (2012), Phys. Rev. Lett. **112**, 019902(E) (2014).

[12] F. Furrer, Phys. Rev. A **90**, 042325 (2014).

[13] M. Berta, F. Furrer, V. B. Scholz, J. Math. Phys. **57**, 015213 (2016).

[14] Cosmo Lupo, Carlo Ottaviani, Panagiotis Papanastasiou, Stefano Pirandola, *Composable Security of Measurement-Device-Independent Continuous-Variable Quantum Key Distribution against Coherent Attacks*, to appear on the arXiv (27 April 2017).

[15] M. Tomamichel, Ph.D. thesis, arXiv:1203.2142.