nature communications

Article

https://doi.org/10.1038/s41467-024-51421-7

Demonstration of microwave single-shot quantum key distribution

Received: 16 February 2024

Accepted: 7 August 2024

Published online: 30 August 2024

Check for updates

Florian Fesquet[1,2] ✉, Fabian Kronowetter[1,2,3], Michael Renger[1,2], Wun Kwan Yam[1,2], Simon Gandorfer[1,2], Kunihiro Inomata[4,5], Yasunobu Nakamura[4,6], Achim Marx[1], Rudolf Gross[1,2,7] & Kirill G. Fedorov[1,2,7] ✉

Security of modern classical data encryption often relies on computationally hard problems, which can be trivialized with the advent of quantum computers. A potential remedy for this is quantum communication which takes advantage of the laws of quantum physics to provide secure exchange of information. Here, quantum key distribution (QKD) represents a powerful tool, allowing for unconditionally secure quantum communication between remote parties. At the same time, microwave quantum communication is set to play an important role in future quantum networks because of its natural frequency compatibility with superconducting quantum processors and modern near-distance communication standards. To this end, we present an experimental realization of a continuous-variable QKD protocol based on propagating displaced squeezed microwave states. We use superconducting parametric devices for generation and single-shot quadrature detection of these states. We demonstrate unconditional security in our experimental microwave QKD setting. The security performance is shown to be improved by adding finite trusted noise on the preparation side. Our results indicate feasibility of secure microwave quantum communication with the currently available technology in both open-air (up to ~ 80 m) and cryogenic (over 1000 m) conditions.

Quantum key distribution (QKD) is a method to securely exchange information between two authenticated remote parties. Contrary to classical encryption relying on computationally asymmetric tasks, the security of QKD protocols is based on quantum mechanical properties. Among the variety of existing QKD protocols, continuous-variable (CV) protocols have been extensively developed due to their technological compatibility with existing classical communication platforms, their ability to deliver high secret key rates over large distances, and less demanding experimental requirements as compared to discrete-variable protocols[1,2]. Contrary to discrete-variable QKD, CV-QKD protocols usually rely on experimentally measurement techniques, such as the homodyne or heterodyne methods, which are less demanding than single-photon detection or counting. In the optical domain, CV-QKD protocols have been successfully implemented within large networks and achieved high secure bit rates[3–6]. In parallel, a tremendous progress has been made in quantum information processing with superconducting circuits operating at microwave frequencies[7–12]. Arguably, this field holds one of the biggest promise to achieve

[1]Walther-Meißner-Institut, Bayerische Akademie der Wissenschaften, Garching, Germany. [2]Physics Department, School of Natural Sciences, Technical University of Munich, Garching, Germany. [3]Rohde & Schwarz GmbH & Co. KG, Munich, Germany. [4]RIKEN Center for Quantum Computing (RQC), Wako, Saitama, Japan. [5]National Institute of Advanced Industrial Science and Technology, Tsukuba, Ibaraki, Japan. [6]Department of Applied Physics, Graduate School of Engineering, The University of Tokyo, Bunkyo-ku, Tokyo, Japan. [7]Munich Center for Quantum Science and Technology (MCQST), Munich, Germany. ✉e-mail: florian.fesquet@wmi.badw.de; kirill.fedorov@wmi.badw.de

scalable quantum computing. Microwave CV-QKD protocols possess a huge potential due to their intrinsic frequency compatibility with superconducting quantum processors, while providing access to unconditionally secure communication. In addition, CV-QKD protocols typically operate with Gaussian states, such as coherent or squeezed states, which can be generated and controlled in the steady-state regime. Recent theoretical studies[13,14] indicate that microwave CV-QKD protocols can be implemented in open-air conditions, potentially complementing short-distance classical communication protocols such as WiFi, Bluetooth. There, microwave communication benefits from a strong resilience to weather conditions, as compared to optical communication[15,16].

A general CV-QKD protocol aims to securely exchange information between a sender (Alice) and a receiver (Bob) using coherent or squeezed states. Information is encoded as a sequence of numbers, referred to as a key, in the q- and p-field quadrature bases of these states. The quantum states propagate through a quantum channel, which is assumed to be under the full control of a malicious eavesdropper (Eve) who tries to syphon information about the key. The security of CV-QKD protocols relies on a single use of each state prepared by Alice, since averaging over multiple copies reveals too much information to Eve. Further details about this protocol can be found in ref. 14. For protocols based on squeezed states, where information is encoded into a single field quadrature, Bob implements single-shot quadrature measurements (SQMs) of the encoding quadrature. In the optical domain, this task is conventionally performed using a homodyne detection technique. In the microwave domain, we achieve an equivalent signal detection using superconducting phase-sensitive amplifiers[17–20].

In this work, we present an experimental realization of a one-way CV-QKD protocol based on the Gaussian modulation of propagating squeezed microwave states[21] in a cryogenic environment. Our experiment serves as a proof-of-principle for microwave CV-QKD protocols and sheds light on their practical limitations. For SQMs, we use a superconducting Josephson parametric amplifier (JPA), which enables strong phase-sensitive amplification and high quantum efficiency well beyond the standard quantum limit[22–24]. We focus on a scenario, where preparation losses and a detection noise are trusted. The quantum channel is an untrusted noisy loss channel, experimentally implemented by a cryogenic directional coupler (highly asymmetric microwave beam splitter) with fixed power losses ε_E and tunable coupled Gaussian noise. The latter is characterized by $\bar{n}$ artificially generated noise photons coupled to the propagating signal. As such, our experiment can be viewed as a quantum simulation of a real CV-QKD implementation, where we controllably vary the temperature of the thermal background in the quantum channel. To prove the security of our protocol, we study the case of a collective Gaussian attack by Eve over the ensemble of states sent by Alice[25]. Our analysis demonstrates a feasibility of unconditionally secure microwave CV-QKD in a cryogenic environment over distances approaching 1200 m, which corresponds to open-air conditions with distances up to 80 m. Owing to the finite length of the exchanged keys, we extend our security analysis by considering both conventional finite-size induced terms[26] and quantum channel parameter estimations[27]. Here, we experimentally demonstrate secure communication for a key length of $N = 16{,}665$ numbers, also commonly referred to as symbols. We find that our experiment allows for an accurate statistical estimation of the channel losses and coupled noise.

Results

Microwave CV-QKD protocol implementation

Our CV-QKD protocol relies on the generation of displaced squeezed microwave states to encode a key from Alice. Each squeezed state is generated by implementing a squeezing operation along the $q-$ or $p-$ quadrature, randomly chosen by Alice, which are to be displaced in phase space to encode Alice's key. In Fig. 1, we illustrate its concept and present the microwave scheme of our experimental implementation. Here, we choose the carrier frequency of all quantum states to be $\omega/2\pi = 5.48$ GHz. We use a superconducting flux-driven JPA for generation of squeezed microwave states, which are characterized by a

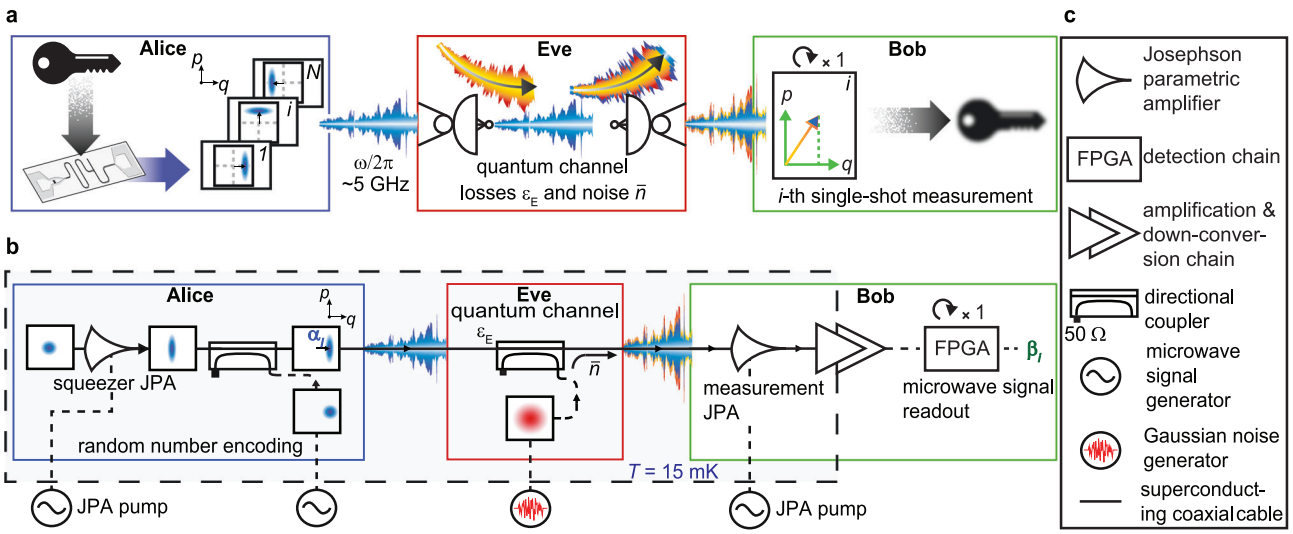

Fig. 1 | General concept of a prepare-and-measure CV-QKD protocol based on displaced squeezed states and its microwave experimental implementation. **a** In the CV-QKD protocol, Alice encodes her key $\mathcal{K}_A = \{\alpha_i\}_{i\in\{1,\ldots,N\}}$ in an ensemble of q- or p-displaced squeezed states. These states propagate as microwave signals through a quantum channel, which is assumed to be under Eve's control and is parametrized by power losses ε_E and an added noise photon number $\bar{n}$. Bob performs SQMs to extract displacement amplitudes of each incoming state, resulting in a measured key $\mathcal{K}_B = \{\beta_i\}_{i\in\{1,\ldots,N\}}$ (see Supplementary Notes 2 and 3). **b** Experimental scheme of the microwave CV-QKD protocol with superconducting JPAs in the cryogenic environment. For each symbol, Alice generates a q- or p-squeezed state which is subsequently displaced using a directional coupler coupled to a strong coherent signal. The resulting state propagates through a quantum channel consisting of a second directional coupler with transmissivity $1-\varepsilon_E = 0.9885$. This coupler is used to inject a variable number of noise photons $\bar{n}$ and, thus, simulate different channel conditions. On Bob's side, a strong phase-sensitive amplification is performed using a second JPA, resulting in the SQM of each received microwave signal. Each of these signals is sampled using a field-programmable gate array (FPGA) to compute a single I/Q point from which the displacement β_i is obtained. Color plots in boxes depict Wigner functions of quantum states in the quadrature phase space (q, p). **c** Legend for various experimental components in (**b**).

squeezing level S below vacuum[28,29]. Our JPAs consist of a coplanar waveguide $\lambda/4$ resonator short-circuited to the ground by a direct current superconducting quantum interference device (dc-SQUID). The dc-SQUID provides a flux-tunable inductance, which allows for frequency tuning of the JPAs. For the generation of squeezed states, our JPAs are operated in the phase-sensitive regime by pumping them at twice their resonance frequencies, $\omega_p = 2\omega$. The squeezed states are subsequently displaced in quadrature phase space using a cryogenic directional coupler[28]. Each displacement operation encodes a symbol α_i drawn from a codebook following a Gaussian distribution with the fixed variance σ_A^2. These symbols constitute Alice's key $\mathcal{K}_A = \{\alpha_i\}_{i\in\{1,\ldots,N\}}$. Displacement operations are performed either along the q or p directions in phase space, chosen randomly for each symbol but always along the same direction as for the squeezing operations. For maximal security, we impose the condition $\sigma_s^2 + \sigma_A^2 = \sigma_{as}^2$, where ($\sigma_{as}^2$) σ_s^2 denotes the (anti-)squeezed quadrature variances, in order to prevent Eve from extracting information on the encoding basis by averaging over the ensemble of Alice's states. In our measurements, we keep a constant average squeezing level S = 3.6(4) dB. Each displaced squeezed state propagates through the quantum channel under Eve's control, implemented in our experiment with a second directional coupler, as illustrated in Fig. 1, adding to incoming states fixed losses ε_E and a tunable coupled noise $\bar{n}$. For signal readout, Bob uses a second JPA to perform the SQMs with a quantum efficiency that depends on the added JPA noise. This noise is related to intrinsic losses, pump-induced noise[11,24], and higher-order nonlinearities[30]. Single-shot measurements, ideally implemented with quantum efficiency close to unity, are obtained with a quantum efficiency well above 50 % and without any averaging of measured signals. The SQM is performed for each symbol encoded by Alice and results in a measured key for Bob $\mathcal{K}_B = \{\beta_i\}_{i\in\{1,\ldots,N\}}$. In practical implementations, a CV-QKD protocol includes additional post-processing. In particular, Bob does not know the encoding basis chosen by Alice. Therefore, Alice and Bob proceed to an additional step, commonly referred to as *sifting*. In this step, Alice discloses which basis she chose once Bob performed all his SQMs, resulting in half the data being discarded. Afterward, Alice and Bob implement a classical error correction algorithm which uses either Alice's or Bob's keys as a reference to provide them with a common key. Here, we consider the direct reconciliation (DR) regime, where Alice's key is used as a reference, known to offer a better resilience to the coupled noise $\bar{n}$ as compared to reverse reconciliation, where Bob's key is taken as the reference[31,32].

Single-shot measurements and correlations

To describe the strong phase-sensitive amplification resulting in SQMs, we use the covariance matrix formalism. When the q quadrature is amplified, we write the covariance matrix of an amplified single-mode state as

$$\mathbf{V}' = \mathbf{J}^T\mathbf{V}\mathbf{J} + \mathbf{N}, \quad \mathbf{J} = \begin{pmatrix} \sqrt{G_J} & 0 \\ 0 & 1/\sqrt{G_J} \end{pmatrix}, \tag{1}$$

where G_J is the degenerate JPA gain and $\mathbf{V}$ is the input covariance matrix. An equation on the p quadrature is obtained by swapping diagonal terms. In addition, $\mathbf{N}$ is a diagonal matrix representing the noise added by our amplification chain. From Eq. (1), we find that the second diagonal element is attenuated by the degenerate gain to $V'_{22} = V_{22}/G_J + N_{22}$. As a result, in the case $G_J \gg 1$, information about the deamplified quadrature becomes inaccessible from SQMs as opposed to the amplified quadrature. Experimentally, we characterize the quadrature amplification noise N_x using the quadrature quantum efficiency defined as $\eta = 1/(1 + 2N_x)$[30]. In Fig. 2b, we show an exemplary normalized histogram of single-shot measurements of Bob's symbols with G_J = 19.1(4) dB and η = 65(2)%. Superimposed to the histogram, we plot an extrapolated quadrature distribution model (see "Methods") which coincides well with our data without any fitting parameters. The model parameters are obtained from independent calibration measurements (see "Methods") of the experimental setup. We show in Fig. 2a an exemplary Wigner function evolution of quantum states in our protocol.

Following these measurements, Bob possesses a set of symbols correlated to the initial set sent by Alice. For the rest of this work, we consider the case where Alice's encoding basis and Bob's measurement basis coincide, effectively implementing the sifting step of the protocol. However, the effect of a realistic sifting is taking into account by adding a 50% multiplier to the secret key rates in the asymptotic limit. We note that sifting leaves the measured mutual information and calculated Holevo quantity unchanged[27]. We characterize these correlations by computing the mutual information (MI) between Alice's encoded key $\mathcal{K}_A$ and Bob's corresponding measured key $\mathcal{K}_B$. For continuous-variable states, the MI, assuming SQMs, is expressed as $I(\mathcal{K}_A : \mathcal{K}_B) = \log_2(1+\mathrm{SNR})/2$, where SNR is the signal-to-noise ratio. In Fig. 2c, we plot the MI extracted from our measurement for the amplified (deamplified) quadrature, denoted as X_B (Y_B). We note that the MI is insensitive to any linear rescaling of either Alice's or Bob's keys and, therefore, captures core correlations between their datasets. For the quadrature X_B, we observe a clearly non-zero MI, indicating strong correlations between Alice's and Bob's key. Conversely, we observe a nearly zero MI for the deamplified quadrature, demonstrating an almost complete loss of information, as expected from the Heisenberg principle for conjugate variables. Additionally, we show values for the MI based on our model under the assumption that Alice's and Bob's keys follow a Gaussian distribution. The accuracy of our model is quantified using the Bhattacharyya coefficient $\mathcal{B}$[33], which evaluates the overlap between measured quadrature distributions and our model predictions. Based on the measurements presented in Fig. 2, we compute $\mathcal{B}(P_e(X_B), P_m(X_B)) = 99.98(1)\%$, where $P_e(X_B)$ is the probability distribution of the measured amplified quadrature X_B and $P_m(X_B)$ is its corresponding model quadrature distribution. For the deamplified quadrature Y_B, this analysis results in $\mathcal{B}(P_e(Y_B), P_m(Y_B)) = 99.87(2)\%$. The $\mathcal{B}$ values close to unity indicate excellent agreement between our model and experimental measurements, which can be interpreted as a proof of genuine single-shot quadrature measurements in our experiments.

Security analysis

In order to extract secret information from their datasets, Alice and Bob estimate an upper bound for the amount of information leaked during the quantum communication using the Holevo quantity χ_E. First, we consider the asymptotic case, where communicated keys are assumed to be infinitely long. In this case, we rely on our calibration measurements to have an exact knowledge about the channel losses and coupled noise and show in Fig. 2c the resulting Holevo quantity. Without loss of generality[25,34], we can assume that Eve employs a collective Gaussian attack[35] with an optimal joint measurement and restrict her attack to an entangling cloner attack[32]. From the perspective of Alice and Bob, the signal coupled by Eve's attack appears as a thermal noise signal with $\bar{n}_{th} = 2\bar{n}/\varepsilon_E$. The security of communication in the asymptotic case is determined by bounding the number of secure bits communicated per symbol K_{exp} with the secret key $K = I(\mathcal{K}_A : \mathcal{K}_B) - \chi_E \le K_{exp}$. In Fig. 3a, we show the secret key K associated with the MI presented in Fig. 2c. We observe a clear positive secret key, which indicates that Alice and Bob share more information than what leaks to Eve, resulting in an unconditional security in the asymptotic regime. More precisely, the secret key remains positive up to 0.062(2) of coupled noise photons. To improve the protocol performance, we can increase the codebook size, squeezing level, or quantum efficiency. However, various limitations, such as compression effects of the JPAs, JPA noise performance, and experimentally achievable squeezing levels, must be taken into account. In our

https://doi.org/10.1038/s41467-024-51421-7

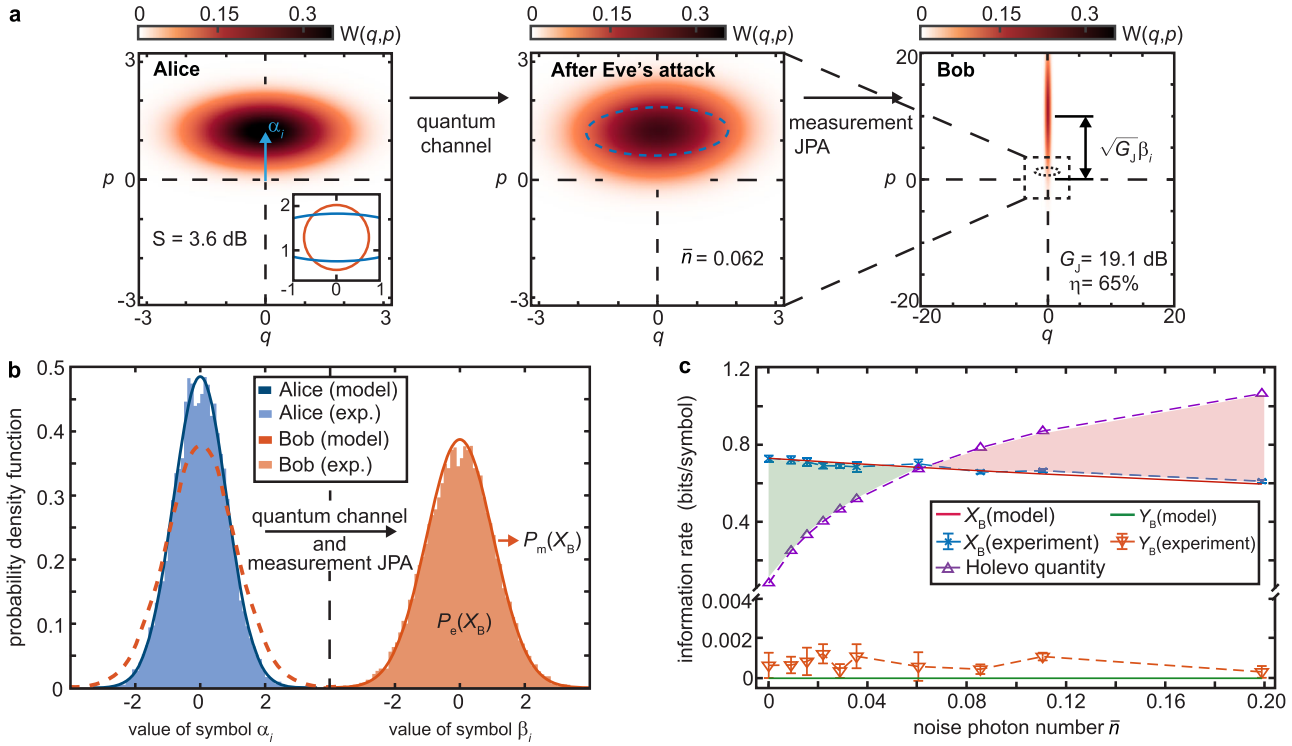

Fig. 2 | Tomography and single-shot measurement histograms of displaced squeezed microwave states. a Exemplary reconstructed Wigner function of the evolution of a quantum key symbol, starting from its preparation at Alice, followed by propagation through the quantum channel while being exposed to losses and noise (Eve's attack), finishing at Bob with a strong phase-sensitive amplification. The inset of the left Wigner function plot shows the 1/e contours for an ideal vacuum (red circle) and experimental squeezed state (blue ellipsoid) indicating squeezing below the level of vacuum fluctuations. **b** Exemplary measured histograms for Alice's and Bob's key symbols. For comparison with the measured probability distribution $P_e(X_B)$, we plot our quadrature model (solid lines) resulting in a zero-mean Gaussian probability distribution $P_m(X_B)$, whose variances are obtained from independent calibration measurements (see "Methods"). **c** MI between Alice's and Bob's keys for the amplified (deamplified) quadrature $X_B(Y_B)$ as a function of the coupled noise photon number $\bar{n}$. We additionally show the MI computed from our model, which is also based on the independent calibration measurements. We emphasize that the model is not a fit of the measurement data. Lastly, we show the corresponding Holevo quantity. The shaded green (red) area on the left (right) represents the region where the MI is larger (smaller) than the Holevo quantity, resulting in a unconditionally secure (insecure) communication. The error bars denote SD of the experimental data.

experiments, we enlarge the codebook variance σ_A^2 by allowing for additional input noise from the first JPA (originating from a pump-induced noise and intrinsic losses) while simultaneously keeping the squeezing level constant. This results in an increase of the anti-squeezing level from 7.1 to 7.6 dB and, hence, in an enhancement of σ_A^2 by ~14%. As shown in Fig. 3a, this increased codebook variance leads to a higher secret key, extending the noise tolerance to 0.071(2) photons. During this 2nd measurement run, we also obtain a slightly higher quantum efficiency of $\eta = 68(2)\%$ as compared to the initial $\eta = 65(2)\%$. However, based on our model, this increase in η alone is insufficient to induce the observed higher secret keys. The increase in secret key values with added preparation noise illustrates a general beneficial effect of adding trusted noise on the reference side of error correction[36,37]. Based on the relation $\sigma_s^2 + \sigma_A^2 = \sigma_{as}^2$, this effect in our protocol leads to a larger increase of the mutual information than the Holevo quantity, and thus, to an increase of the secret key rate. For the case of the lowest coupled noise, $\bar{n} \simeq 2 \times 10^{-6}$ (given by the coupling to our sample stage at $T \simeq 15$ mK), we measure a relatively high secret key up to 0.74 bits/symbol and a corresponding SNR of 2.16, similar to optical implementations in long-distance communication[38].

Our security analysis can be extended to include limiting effects arising from the finite size of the transmitted key[26]. These finite-size effects, inducing a decrease of the secret key, are reflected by additional finite-size terms Δ (see Supplementary Note 8). Equally important, in practical QKD implementations, Alice and Bob are unaware of the exact quantum channel parameters and must estimate them using part of the communicated key. To achieve maximal security, the channel parameters are obtained from worst-case-scenario statistical estimators ε_E^* and $\bar{n}^*$ for the channel losses ε_E and coupled noise $\bar{n}$, respectively. Following the approach in ref. 13, the secret key bound takes the form $r[\beta I(\mathcal{K}_A : \mathcal{K}_B) - \chi_E(\varepsilon_E^*, \bar{n}^*) - \Delta(n_{exp})] \leq K_{exp}$, where $r = n_{ec} p_{ec}/N$ is a rescaling prefactor with n_{ec} denoting the fraction of the exchanged key not used for parameter estimation. The efficiency of the error correction protocol is denoted as β and its success probability p_{ec}, with an achievable $\beta > 90\%$[39] for an SNR around unity. As illustrated in Fig. 3a, if we account only for the finite-size terms Δ, we can observe a region of positive secret key up to $\bar{n} = 0.004$ ($\bar{n} = 0.009$) for the 1st run (2nd run). These effects can be largely mitigated by extending the key length to a more demanding but realistic value of $N \geq 10^6$. From our experimental keys, we compute a worst-case unbiased estimator for the losses and noise as $\varepsilon_E^* = \hat{\varepsilon}_E + w\sigma_{\hat{\varepsilon}_E}$ and $\bar{n}^* = \hat{\bar{n}} + w\sigma_{\hat{\bar{n}}}$, with unbiased estimators $\hat{\varepsilon}_E$ and $\hat{\bar{n}}$, built using $N - n_{ec}$ symbols of Alice's and Bob's key. Here, w is a confidence parameter for a chosen error ε_{ec}, reducing to $w = \sqrt{2}\,\mathrm{erf}^{-1}(1 - 2e_{ec})$. Considering an error of $e_{ec} = 10^{-3}$ and not accounting for the finite-size terms Δ, we vary the fraction $N - n_{ec}$ to build the estimators leading to a positive secret key up to roughly $\bar{n} = 0.012$ ($\bar{n} = 0.017$) for the 1st run (2nd run). We conclude that all finite-size effects can be straightforwardly solved by increasing the key length to $N \geq 10^6$.

Finally, to provide a more application-oriented outlook, we estimate maximal communication distances the microwave CV-QKD protocol could achieve with the current experimental performance. To this end, we consider a communication protocol, where Alice and Bob keep the same experimental parameters as in the 2nd run, except for

https://doi.org/10.1038/s41467-024-51421-7

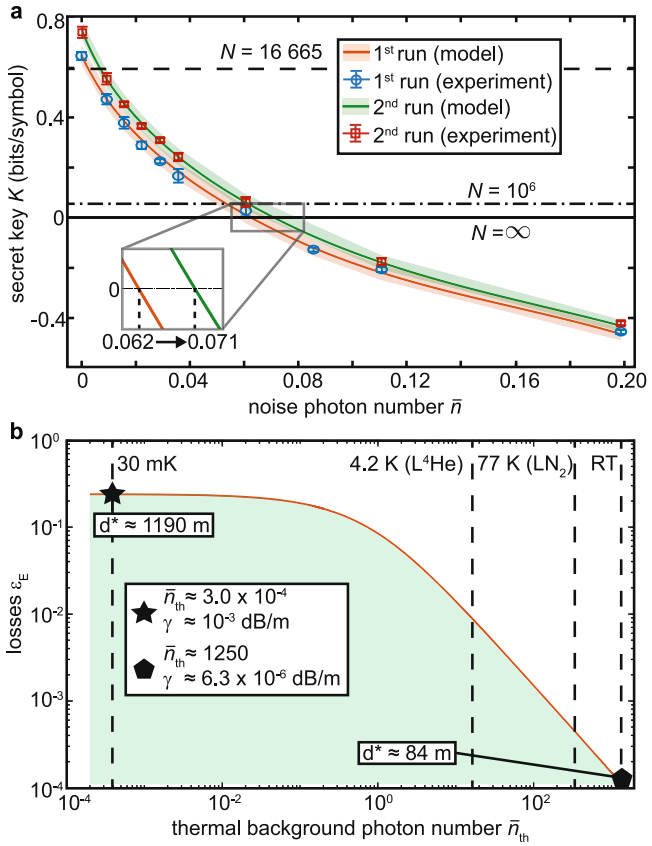

Fig. 3 | Secret key of the microwave CV-QKD protocol. a Measured secret key of the CV-QKD protocol for two experimental runs: 1st with squeezing (anti-squeezing) levels of 3.6 (7.1) dB and 2nd with squeezing (anti-squeezing) levels of 3.6 (7.6) dB. The dashed lines represent the finite-size terms, which impose lowered noise cut-offs for reaching the unconditional security. The error bars and shaded areas denote SD of the experimental data and model, respectively. **b** Estimation of maximally tolerable losses (solid line) for positive secret keys as a function of the photon number in the thermal background, $\bar{n}_{\mathrm{th}}$. This analysis is based on the experimental data from the 2nd run. The green shaded area indicates the region of positive (i.e., secure) secret keys. We emphasize two particular temperatures on this curve: the cryogenic temperature ~30 mK and room temperature (RT) ~ 300 K. At millikelvin temperatures, we assume characteristic losses in superconducting cables of $\gamma = 1.0 \times 10^{-3}$ dB/m while for the open-air conditions, we restrict ourselves to atmospheric microwave losses $\gamma = 6.3 \times 10^{-6}$ dB/m due to pure absorption. Under these conditions, we estimate the maximum communication distance, $d^* \simeq 1190$ m at 30 mK and $d^* \simeq 84$ m at 300 K. For the open-air scenario, we neglect possible path losses, assuming those can be fully compensated by appropriate antennae, and focus on unavoidable physical limitations.

modified losses ε_{E} and noise photon numbers $\bar{n} = \bar{n}_{\mathrm{th}}\varepsilon_{\mathrm{E}}/2$ of the quantum channel. In Fig. 3b, we show maximally tolerable losses for a given photon number $\bar{n}_{\mathrm{th}}$. We find that the unconditionally secure microwave communication up to 1190 m is feasible in a fully cryogenic environment at $T \simeq 30$ mK based on commercial superconducting cables with characteristic losses of ~10^{-3} dB/m[40], making microwave CV-QKD relevant for secure local area quantum networks[41]. In a cryogenic environment further, proof-of-principle, experiments can be implemented using a several meter long spool of the superconducting cable. Alternatively, one can rely on the already existing cryogenic links[42,43] to verify the CV-QKD microwave protocols over distances up to several tens of meters. There, it is also possible to employ microwave waveguides, which might offer even lower attenuation losses[40], as compared to superconducting coaxial cables while not as flexible as them. We also find that the unconditionally secure microwave communication should be possible up to 84 m in the open-air environment with $\bar{n}_{\mathrm{th}} \simeq 1250$ for signals at $\omega/2\pi \simeq 5$ GHz. This finding results from considering the very low microwave atmospheric absorption losses of 6.3×10^{-6} dB/m in clear weather conditions[14]. Furthermore, we estimate a path loss for the possible communication distance of 84 m of ~80 dB. A typical parabolic antenna with a diameter of around 2 m provides gain around 40 dB[14], implying that a pair (as an emitter and a receiver, Alice and Bob) of such antennae would fully compensate the considered path loss. In this context, implementation of a low-loss and sufficiently broadband interface between the cryogenic part and the antennae remains an important technological challenge for the future. Therefore, we focus on fundamentally unavoidable physical limitations due to absorption losses and treat the estimated communication distance as an upper bound for unconditionally secure microwave QKD based on the performance of our existing JPAs. We note that the presence of a finite uncompensated path loss does not necessarily prevent secure communication but may reduce the secure communication distances. As such, microwave CV-QKD demonstrates a notable potential for secure short-range open-air microwave communication, where microwave signals additionally benefit from a resilience to weather imperfections[14].

Discussion

Our experiments reveal that the main limiting factor of the performance of the microwave CV-QKD protocol is the total noise, which is composed of the coupled noise and the amplification noise. Another limitation is the codebook size, which can be increased by adding trusted noise on Alice's side or by increasing the initial squeezing level. This approach is limited by compression effects of our JPAs, which typically set on at input signal powers around −130 dBm. Traveling-wave parametric amplifiers[44] could serve as alternative phase-sensitive amplifiers in future experiments, commonly tolerating higher input powers with quantum efficiencies comparable to our JPAs. Their broadband amplification properties also enable the implementation of frequency multiplexing techniques, which deliver significantly higher secure bit rates.

Our experiments show that SQMs implemented with phase-sensitive amplifiers can be considered as a microwave equivalent of optical homodyne detection. More precisely, our experiment demonstrates the possibility of using these SQMs to unravel properties of quantum states, particularly relevant for quantum state tomography[20,45]. This approach can be further extended to non-Gaussian state tomography and complements error correction codes by offering a single-shot quadrature detection technique[46,47]. Lastly, we extrapolate an experimental secret key rate of 42 kbit/s in our CV-QKD realization. By using the Shannon-Hartley theorem with our measurement bandwidth of 400 kHz, we estimate an upper bound of our raw secret key rate up to 152 kbit/s for the 2nd run, paving the way for secure high-bit-rate microwave CV-QKD communication. We find that these key rates are mainly limited by the phase stabilization of our JPAs (see "Methods") which could be minimized in future experiments by using better frequency filtering in our experimental setup and additional magnetic shielding. Increasing the measurement bandwidth results in an initial increase of the secret key rate at the cost of a larger background noise. To remedy this problem, various multiplexing approaches, such as time, frequency, or code-division multiplexing methods, can be used. These approaches may require technical improvements of the JPAs, e.g., enlarged instantaneous bandwidths and saturation powers. Secret key rates can be further increased by extending the codebook size via adding an extra trusted preparation noise or using larger squeezing levels. Similarly, improving the quantum efficiency of the measurement JPA would greatly increase the final secret key rate. Our demonstrated results promote the ongoing development of local microwave networks[41,43], where short-distance secure microwave quantum communication platforms could complement current classical microwave communication technologies such

as Wifi and Bluetooth due to the intrinsic frequency and range compatibilities.

Methods

Experimental squeezed microwave states

We experimentally generate squeezed states with JPAs, which are flux-tunable superconducting devices consisting of a harmonic $\lambda/4$ resonator shorted to ground with a dc-SQUID made of Al/AlO_X/Al Josephson junctions. These JPAs are operated in the phase-sensitive regime pumping them with strong coherent microwave tones. The squeezed states are described using the squeeze operator $\hat{S} = \exp((\xi^* \hat{a}^2 - \xi(\hat{a}^\dagger)^2)/2)$, where $\hat{a} = \hat{q} + i\hat{p}$ ($\hat{a}^\dagger = \hat{q} - i\hat{p}$) is the annihilation (creation) operator with the quadrature operators $\hat{q}$ and $\hat{p}$ such that $[\hat{q}, i\hat{p}] = 1/2$ and $\xi = re^{i\varphi}$ is the complex squeezing amplitude. Here, the phase $\varphi = -2\gamma$ is related to the squeezing angle γ between the anti-squeezed quadrature and the p quadrature in the quadrature phase space. In addition, r represents the squeeze factor, related to the amount of squeezing. The latter is quantified using the squeezing level $S = -10\log_{10}(\sigma_s^2/0.25)$. Similarly, we define the anti-squeezing level $A = 10\log_{10}(\sigma_{as}^2/0.25)$. In our measurements, we implement a phase-locked loop with a feedback, which periodically adjusts the phase of our pump tones to maintain a stable squeezing angle[48].

Quadrature model and calibration measurements

The microwave CV-QKD protocol is modeled by describing each element presented in the experimental schematic in Fig. 1 with a corresponding operator. The squeezing operation from the first JPA is described by a squeeze operator $\hat{S}_A$. Each directional coupler is modeled with a beam splitter operator, $\hat{C}_A$ and $\hat{C}_E$, and their associated power transmissivity, τ_A and $\tau_E = 1 - \varepsilon_E$, respectively. For the measurement JPA, we use a noisy squeeze operator, $\hat{S}_B'$, to account for the added noise $\bar{n}_J$ of the JPA. Since we are considering single-shot measurements, we also include the HEMT amplifier, described by an amplification operator $\hat{H}$ to account for an amplification noise N_H. Additionally, we introduce path losses in between each component which are described by a beam splitter operator $\hat{L}_i$ for $i \in \{1, 2, 3, 4\}$. The final output state after the HEMT can be expressed as

$$\begin{aligned} \hat{\rho}_{out} &= \hat{T}\hat{\rho}_{in}\hat{T}^\dagger, \\ \hat{T} &= \hat{H}\hat{L}_4\hat{S}_B'\hat{L}_3\hat{C}_E\hat{L}_2\hat{C}_A\hat{L}_1\hat{S}_A, \end{aligned} \tag{2}$$

where $\hat{\rho}_{in}$ is the overall input state of our experimental setup, accounting for signal modes and all other modes involved with the action of the operators. All experimental parameters used in Eq. (2) are extracted from independent calibration measurements, where we perform full Wigner tomography of the measured signals, under the assumption that all quantum states are Gaussian, to obtain the parameters individually (see Supplementary Note 7). The accuracy of our tomography method relies on a precise photon number calibration performed using Planck spectroscopy measurements[49]. Wigner function tomography is performed using a reference state tomography based on measured quadrature moments associated with a to-be-reconstructed quantum state[29,50].

Holevo quantity

The Holevo quantity of Eve, giving an upper bound on her accessible information about Alice's key, is computed as

$$\chi_E = S_N\left(\int_A d\alpha f_A(\alpha)\hat{\rho}_{E,\alpha}\right) - \int_A d\alpha f_A(\alpha) S_N(\hat{\rho}_{E,\alpha}), \tag{3}$$

by integrating over the ensemble of states, $\{\hat{\rho}_{E,\alpha} | \alpha \in A\}$, with A being the codebook ensemble of Alice and individual density matrices $\hat{\rho}_{E,\alpha}$, obtained by Eve using the entangling cloner attack. The function f_A represents the probability density function of Alice's random variable. Here, the integral is taken over the ensemble of displacements that Alice can use during the communication and S_N is the von Neumann entropy. We note that the function f_A describing the displacement choice of Alice is a Gaussian function, therefore all states involved in computation of the Holevo quantity are also Gaussian. A more detailed description of the computation of the Holevo quantity can be found in Supplementary Note 6.

Data availability

Data that support the findings of this study are available from the corresponding author upon request.

Code availability

The code used for data analysis and visualization is available from the corresponding author upon request.

References

1. Xu, F., Ma, X., Zhang, Q., Lo, H.-K. & Pan, J.-W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **92**, 025002 (2020).
2. Pirandola, S. et al. Advances in quantum cryptography. *Adv. Opt. Photon.* **12**, 1012–1236 (2020).
3. Peev, M. et al. The SECOQC quantum key distribution network in Vienna. *New J. Phys.* **11**, 075001 (2009).
4. Liao, S.-K. et al. Satellite-to-ground quantum key distribution. *Nature* **549**, 43–47 (2017).
5. Chen, J.-P. et al. Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas. *Nat. Photonics* **15**, 570–575 (2021).
6. Wang, S. et al. Twin-field quantum key distribution over 830-km fibre. *Nat. Photonics* **16**, 154–161 (2022).
7. Arute, F. et al. Quantum supremacy using a programmable superconducting processor. *Nature* **574**, 505–510 (2019).
8. Bienfait, A. et al. Phonon-mediated quantum state transfer and remote qubit entanglement. *Science* **364**, 368–371 (2019).
9. Pogorzalek, S. et al. Secure quantum remote state preparation of squeezed microwave states. *Nat. Commun.* **10**, 2604 (2019).
10. Kjaergaard, M. et al. Superconducting qubits: current state of play. *Annu. Rev. Condens. Matter Phys.* **11**, 369–395 (2020).
11. Fedorov, K. G. et al. Experimental quantum teleportation of propagating microwaves. *Sci. Adv.* **7**, eabk0891 (2021).
12. Kronowetter, F. et al. Quantum microwave parametric interferometer. *Phys. Rev. Appl.* **20**, 024049 (2023).
13. Pirandola, S. Composable security for continuous variable quantum key distribution: trust levels and practical key rates in wired and wireless networks. *Phys. Rev. Res.* **3**, 043014 (2021).
14. Fesquet, F. et al. Perspectives of microwave quantum key distribution in the open air. *Phys. Rev. A* **108**, 032607 (2023).
15. Zhao, Z. & Wu, Z. Millimeter-wave attenuation due to fog and clouds. *J. Infrared Millim. Terahertz Waves* **21**, 1607–1615 (2000).
16. Kaushal, H., Jain, V. & Kar, S. *Free Space Optical Communication*, Vol. 7 (Springer, 2018).
17. Yurke, B. et al. Observation of parametric amplification and deamplification in a Josephson parametric amplifier. *Phys. Rev. A* **39**, 2519–2533 (1989).
18. Castellanos-Beltran, M. A., Irwin, K. D., Hilton, G. C., Vale, L. R. & Lehnert, K. W. Amplification and squeezing of quantum noise with a tunable Josephson metamaterial. *Nat. Phys.* **4**, 929–931 (2008).
19. Eichler, C., Bozyigit, D. & Wallraff, A. Characterizing quantum microwave radiation and its entanglement with superconducting qubits using linear detectors. *Phys. Rev. A* **86**, 032106 (2012).

20. Mallet, F. et al. Quantum state tomography of an itinerant squeezed microwave field. *Phys. Rev. Lett.* **106**, 220502 (2011).
21. Cerf, N. J., Lévy, M. & Assche, G. V. Quantum distribution of Gaussian keys using squeezed states. *Phys. Rev. A* **63**, 052311 (2001).
22. Yamamoto, T. et al. Flux-driven Josephson parametric amplifier. *Appl. Phys. Lett.* **93**, 042510 (2008).
23. Zhong, L. et al. Squeezing with a flux-driven Josephson parametric amplifier. *New J. Phys.* **15**, 125013 (2013).
24. Renger, M. et al. Beyond the standard quantum limit for parametric amplification of broadband signals. *NPJ Quantum Inf.* **7**, 160 (2021).
25. García-Patrón, R. & Cerf, N. J. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.* **97**, 190503 (2006).
26. Leverrier, A., Grosshans, F. & Grangier, P. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A* **81**, 062343 (2010).
27. Laudenbach, F. et al. Continuous-variable quantum key distribution with Gaussian modulation-the theory of practical implementations. *Adv. Quantum Technol.* **1**, 1800011 (2018).
28. Fedorov, K. G. et al. Displacement of propagating squeezed microwave states. *Phys. Rev. Lett* **117**, 020502 (2016).
29. Menzel, E. P. et al. Path entanglement of continuous-variable quantum microwaves. *Phys. Rev. Lett.* **109**, 250502 (2012).
30. Boutin, S. et al. Effect of higher-order nonlinearities on amplification and squeezing in Josephson parametric amplifiers. *Phys. Rev. Appl.* **8**, 054030 (2017).
31. Grosshans, F. et al. Quantum key distribution using Gaussian-modulated coherent states. *Nature* **421**, 238–241 (2003).
32. Grosshans, F., Cerf, N. J., Wenger, J., Tualle-Brouri, R. & Grangier, P. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. *Quantum Info. Comput.* **3**, 535–552 (2003).
33. Fuchs, C. & van de Graaf, J. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Trans. Inf. Theory* **45**, 1216–1227 (1999).
34. Renner, R. & Cirac, J. I. de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Phys. Rev. Lett.* **102**, 110504 (2009).
35. Pirandola, S., Braunstein, S. L. & Lloyd, S. Characterization of collective Gaussian attacks and security of coherent-state quantum cryptography. *Phys. Rev. Lett.* **101**, 200504 (2008).
36. García-Patrón, R. & Cerf, N. J. Continuous-variable quantum key distribution protocols over noisy channels. *Phys. Rev. Lett.* **102**, 130501 (2009).
37. Usenko, V. C. & Filip, R. Trusted noise in continuous-variable quantum key distribution: A threat and a defense. *Entropy* **18**, 20 (2016).
38. Jouguet, P., Kunz-Jacques, S. & Leverrier, A. Long-distance continuous-variable quantum key distribution with a Gaussian modulation. *Phys. Rev. A* **84**, 062317 (2011).
39. Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P. & Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat. Photonics* **7**, 378–381 (2013).
40. Kurpiers, P., Walter, T., Magnard, P., Salathe, Y. & Wallraff, A. Characterizing the attenuation of coaxial and rectangular microwave-frequency waveguides at cryogenic temperatures. *EPJ Quantum Technol.* **4**, 8 (2017).
41. Awschalom, D. et al. Development of quantum interconnects (quics) for next-generation information technologies. *PRX Quantum* **2**, 017002 (2021).
42. Magnard, P. et al. Microwave quantum link between superconducting circuits housed in spatially separated cryogenic systems. *Phys. Rev. Lett.* **125**, 260502 (2020).
43. Yam, W. K. et al. Cryogenic microwave link for quantum local area networks. Preprint at https://arxiv.org/abs/2308.12398 (2024).
44. Macklin, C. et al. A near-quantum-limited Josephson traveling-wave parametric amplifier. *Science* **350**, 307–310 (2015).
45. Knyazev, E., Spasibko, K. Y., Chekhova, M. V. & Khalili, F. Y. Quantum tomography enhanced through parametric amplification. *New J. Phys.* **20**, 013005 (2018).
46. Gottesman, D., Kitaev, A. & Preskill, J. Encoding a qubit in an oscillator. *Phys. Rev. A* **64**, 012310 (2001).
47. Hanamura, F. et al. Single-shot single-mode optical two-parameter displacement estimation beyond classical limit. Preprint at https://arxiv.org/abs/2308.15024 (2023).
48. Fedorov, K. G. et al. Finite-time quantum entanglement in propagating squeezed microwaves. *Sci. Rep.* **8**, 6416 (2018).
49. Gandorfer, S. et al. Two-dimensional Planck spectroscopy. Preprint at https://arxiv.org/abs/2308.02389 (2023).
50. Eichler, C. et al. Observation of two-mode squeezing in the microwave frequency domain. *Phys. Rev. Lett.* **107**, 113601 (2011).

Acknowledgements

The authors acknowledge the contributions of Philipp Krüger and Valentin Weidemann. We acknowledge support by the German Research Foundation via Germany's Excellence Strategy (EXC-2111-390814868), the German Federal Ministry of Education and Research via the project QUARATE (Grant No. 13N15380), the project QuaMToMe (Grant No. 16KISQ036), the Japan Society for the Promotion of Science (JSPS) KAKENHI (Grant No. 22H04937) and the JST Exploratory Research for Advanced Technology (ERATO), Japan (Grant No. JPMJER1601). This research is part of the Munich Quantum Valley, which is supported by the Bavarian state government with funds from the Hightech Agenda Bayern Plus.

Author contributions

K.G.F. planned the experiment. F.F., F.K., and K.G.F. performed the measurements and analyzed the data. M.R., W.K.Y., and S.G. contributed to the development of the measurement software and experimental setup. F.F., F.K., and M.R. developed the theory model. K.I. and Y.N. provided the JPA samples. A.M. contributed to the development of the cryogenic setup. K.G.F. and R.G. supervised the experimental part of this work. F.F. and K.G.F. wrote the manuscript. All authors contributed to discussions and proofreading of the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41467-024-51421-7.

Correspondence and requests for materials should be addressed to Florian Fesquet or Kirill G. Fedorov.

Peer review information *Nature Communications* thanks Neel Kanth Kundu and the other, anonymous, reviewer(s) for their contribution to the peer review of this work. A peer review file is available.