Pflitsch, M.; Kirsanov, N. S.; Perelshtein, M. R.; Vinokur, V. M.; Lesovik, G. B.

Terra quantum at MIPT-QUANT 2020

Published in:
MIPT (PHYSTECH) - QUANT 2020

DOI:
10.1063/5.0054886

Published: 16/06/2021

Document Version
Publisher's PDF, also known as Version of record

Please cite the original version:
Pflitsch, M., Kirsanov, N. S., Perelshtein, M. R., Vinokur, V. M., & Lesovik, G. B. (2021). Terra quantum at MIPT-QUANT 2020. In G. Lesovik, V. Vinokur, & M. Perelshtein (Eds.), *MIPT (PHYSTECH) - QUANT 2020* Article 020001 (AIP Conference Proceedings; Vol. 2362). American Institute of Physics. https://doi.org/10.1063/5.0054886

Terra quantum at MIPT-QUANT 2020

Cite as: AIP Conference Proceedings **2362**, 020001 (2021); https://doi.org/10.1063/5.0054886
Published Online: 16 June 2021

M. Pflitsch, N. S. Kirsanov, M. R. Perelshtein, V. M. Vinokur, and G. B. Lesovik

Terra Quantum at MIPT-QUANT 2020

M. Pflitsch,[1] N. S. Kirsanov,[1, 2, 3] M. R. Perelshtein,[1, 2, 3] V. M. Vinokur,[1, a)] and G. B. Lesovik[1, 2]

[1)]*Terra Quantum AG, St. Gallerstrasse 16A, 9400 Rorschach, Switzerland*

[2)]*Moscow Institute of Physics and Technology, 141700, Institutskii Per. 9, Dolgoprudny, Moscow Distr., Russian Federation*

[3)]*QTF Centre of Excellence, Department of Applied Physics, Aalto University School of Science, P.O. Box 15100, FI-00076 AALTO, Finland*

[a)]*Corresponding author: vv@terraquantum.swiss*

Abstract. Implementations of quantum information-processing systems require quantum algorithms and corresponding material tools to solve problems posited by modern information technologies. Terra Quantum offers state-of-the-art solutions that pave the way to a new level of efficiency in information processing. In this paper, we outline the research activities carried out by Terra Quantum experts who focus on quantum computing and quantum machine learning, sensors and metrology, quantum cryptography, random number generators, and algorithmic cooling.

The "quantum" term surfaced in the late 20th century as a term for something so enormous and important – and referring to scientific connotations – that the common means of admiration felt insufficient. Those of the older generation remember the 90's TV series "Quantum Leap" depicting an overwhelming time-traveling adventure advancement. Now entering what we call the "quantum era" or "quantum revolution era" the air of an over the significance of the term harnesses with its mathematical scientific precision. The exemplary concept that is now central to the media and the scientific lore is "quantum computing." Technological advances have reached such a level that this area now has the potential to become not only an outstanding science and technology – as a result of the first quantum revolution but also – as an outcome of a second quantum revolution – an enormous and overwhelming global business. Among business directions, quantum computing is a sustainable area to invest in because there is no fundamental question as to whether it works—it just does. Remarkably, given an apparent failure of the traditional scientific institutions in providing the technological progress required by the needs of modern society, we come up with the new model of scientific affairs. In this model, the scientific advance is harnessed and intertwined with the investments into business in its traditional sense. A marked example of the success of such a novel approach is again quantum computing: the first really working quantum computers were created not in universities, academic institutions, or national laboratories but in companies like IBM or Google.

Inspired by this success there appeared a diversity of start-ups often associated with the leading university or institutions pursuing a wealth of scientific directions encouraged by the IBM/Google "quantum advance."

Europe has a great tradition as soil for quantum physics. About 100 years ago great European thinkers in the field such as Planck, Schrödinger, Born, Heisenberg, Einstein, Dirac, and many others created what is known now as quantum mechanics. We feel strongly that Europe now is on the verge of the next quantum leap to realize its outstanding scientific potential in the field of quantum technology. Our Conference is an important step in this direction. It invites and represents not only leading scientific experts and institutions but also two of the most energetically developing and dynamic startups specializing in the field, IQM from Finland and the Swiss Terra Quantum. We represent Terra Quantum which is an exemplary institution belonging to a new emergent generation of business formations combining intense business practicing with the initiation of a global ecosystem led by Europe's leading thinkers and experts in this field. We anticipate that the structure of Terra Quantum will most successfully support successful and dynamic business development while providing a perfect interface for transferring the cutting edge scientific and technological advances into industrial and business success. To that end, we bring together the best of researchers in the fields of theoretical physics, quantum information, classical math, machine learning, and, at the same time, engineers, technologists, and business experts. This will create a unique formation harnessing various but intertwined competencies into an unprecedentedly synergistic quantum technology company.

This year's International MIPT-QUANT Conference continuing a chain of International Quantum Information Science meetings anchored at MIPT is supported and co-organized by Terra Quantum. The Conference offers a remarkable forum for the representative list of scientific achievements that marked the first stage of Terra Quantum activity. The main directions that constitute our present focus are as follows.

MIPT (PhysTech) - QUANT 2020
AIP Conf. Proc. 2362, 020001-1–020001-6; https://doi.org/10.1063/5.0054886
Published by AIP Publishing. 978-0-7354-4102-6/$30.00

QUANTUM COMPUTING AND QUANTUM MACHINE LEARNING

As quantum technologies continue to improve theoretically and experimentally, it becomes crucial to understand which modern problems can be addressed using current quantum devices. The scientific community is at the beginning of embracing the capabilities of quantum computers; still, we already know that data processing using quantum phenomena can be exponentially more efficient than classical approaches. However, future computational schemes will not eliminate classical computers: humankind reach significant milestones with classical devices proved the efficiency of these machines in specific problems. At Terra Quantum, we understand that quantum computers are at an early, noisy intermediate-scale stage; thus, much of our research combines classical approaches and quantum algorithms in a hybrid way. We establish state-of-the-art quantum cloud QMWare that consolidates high-performance classical computing, hybrid quantum computing, and machine learning [1].

The main idea behind hybrid quantum computing is the following: utilizing of classical resources to find a problem's hardcore and delegation to the quantum processor unit or implementation of a quantum solution, whose bottlenecks would be eliminated by classical improvements. QMWare anticipates that both these approaches lead to disruptive applications in the most demanding computational problems.

At QMWare, we develop quantum machine learning tools that both enhance machine learning with quantum effects and improve quantum technologies with artificial intelligence. We believe that quantum technologies will massively assist the most advanced machine learning frameworks. Highly autonomous systems that outperform humans at most economically valuable work require large computational resources, limiting their performance.

The hybrid classical-quantum solvers implemented in a quantum/classical computational networks are considerably more efficient to train and, therefore, make predictions. There are several approaches in this direction. Firstly, quantum computing models potentially improves the training process of existing classical models [2, 3, 4]. One can find better extreme points in a objective function landscape or the same optima with fewer iterations. These methods allows for polynomial speedups which is crucial for large complex problems where small improvements gives noticeable gain. Besides, the resent experiments show that quantum models can sample intricate probability distributions in a polynomial time [5], while the same classical sampling could be exponentially difficult. Among many other methods, the most promising are quantum neural networks [6, 7] and quantum kernels [8] that are expected to beat classical models with current noisy quantum devices.

At the same time, classical machine learning has revealed that deep learning networks are capable of identifying complex patterns and trends in data. It would not be possible without powerful computers and special-purpose hardware capable of implementing deep networks with billions of parameters [9]. If machine learning could improve quantum devices, the potential for this impact is colossal.

There are several paths towards such an improvement. The well-known procedure, that could be refined classically, is quantum state tomography, where a quantum state is learned from measurement. In superconducting circuits, one way to improve measurement fidelity is to utilize quantum limited amplifiers [10]. However, these devices often do not provide enough level of accuracy in the qubit's state discrimination. On the other hand, the state discrimination could be performed using machine classification methods with both supervised and unsupervised learning [11].

Other applications include learning Hamiltonians [12], which is very important for statistical physics and automatic generation of quantum experiments [13]. The latter is motivated by the unknown reachability of various configurations in quantum experiments. For instance, in Ref. 14 we realize the machine learning system that autonomously reveals experimental methods which are too complicated for human mind to discover. This work shows that machine learning can offer dramatic advances in how complicated experiments are generated.

METROLOGY (SENSORS)

After Peter Shor invented a quantum algorithm for integer factorization, promising to solve the problem exponentially faster than any classical factoring algorithm, a wealth of solutions based on quantum effects emerged targeting classically intractable problems. One of these tasks, improving the accuracy of measurements, is a key issue for the development of physics and technology. While the fundamental limit of classical measurement schemes is set by the shot noise level, recent advances in quantum hardware resulted in novel approaches based on quantum phenomena that enable to overcome noise tyranny. Technically, quantum protocols provide a signal-to-noise ratio advantage over that of the optimum classical methods. One of the most striking examples, the quantum illumination [15], successfully utilizes the bipartite entanglement in the detection in the presence of high levels of noise and loss. The further improvement of the measurement accuracy can be achieved with the help of multipartite entanglement, e.g., using

NOON photon states in optics [16]. However, these states are difficult to create in general and they typically have a short coherence time. Alternatively, one can reach the quantum speedup without exploiting entanglement, by using the coherence of the wavefunction of a single quantum system as a dynamical resource.

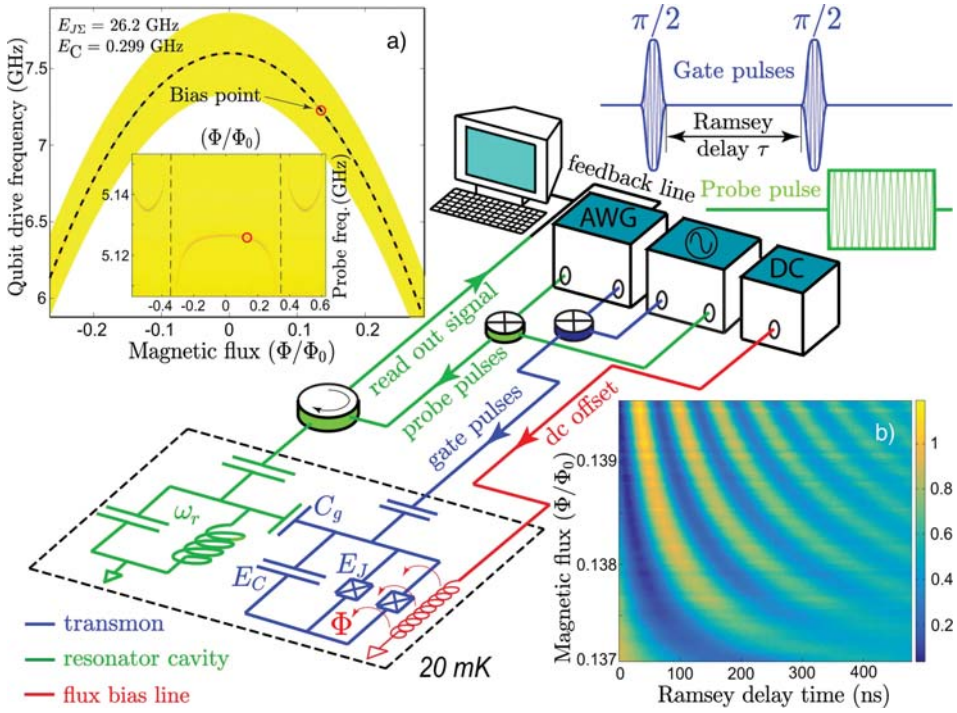

FIGURE 1. Quantum-enhanced magnetometry by phase estimation algorithms with a single superconducting qubit [17]. The schematic shows a transmon qubit (in blue) comprised of a capacitor and a SQUID loop with two nearly identical junctions. The qubit is coupled via a gate capacitor C_g to a coplanar waveguide resonator (CPW, in green). The magnetic flux through the transmon's SQUID loop is controlled by a dc-current flowing through a flux-bias line (in red). **a.** Qubit transition frequency as a function of magnetic flux (parabolic curve). The bottom inset shows the CPW resonator's spectrum. The red circles indicate the bias point of our transmon sensor: we operate far away from the 'sweet spot' in a regime where the transmon's frequency is an approximately linear function of the flux. **b** A pre-measured sample-specific Ramsey interference fringes pattern.

The phase estimation is a natural concept in quantum metrology, where the evaluation of an unknown parameter x is performed through the Hamiltonian of a probe quantum system, where x defines system's energy states $E_n(x)$. In a classical measurement, the precision δx is restricted by the shot-noise limit $\delta x \sim 1/\sqrt{t}$, where t is the measurement time and represents the utilized resource. Nevertheless, this is not a fundamental limit: in the optimal sensing procedures the precision scales as $\delta x \sim 1/t$ constrained only by the Heisenberg relation $\Delta E(x) \geq 2\pi\hbar/t$, where $\Delta E(x)$ is the energy difference.

As one of the most practical example, the Kitaev- [18, 19] and Fourier-transform- [20] quantum algorithms, in combination with coherent superconducting circuits [21] utilized as sensors, proved to be Heisenberg limited in magnetometry. The basic concept of a magnetic-field sensor based on a spin interacting with the field has evolved into experimentally realizable devices based on charge and flux qubits [22, 23, 24]. At Terra Quantum, we investigate a multilevel superconducting device as a magnetic-flux sensor, see Ref. 25, and realize quantum metrological algorithms in Ref. 17 in order to push the measurement sensitivity beyond the standard shot-noise limit. In our experiments, we utilize the coherent dynamics of the quantum artificial atom as a quantum resource.

Importantly, since mentioned protocols do not utilize quantum entanglement, they may be implemented on the systems that shows wave yet classical behavior. Methods spied from quantum metrology can be applied to the classical optical measurements [26, 27, 28, 29], which, in particular, can be used to measure the position, velocity, and displacement of physical objects. In Ref. [30] we construct a complex linear-optic-based device for the Fourier-based phase estimation protocol; the metrological potential of such multiple-beam schemes can be seen in the LIGO optical gravitational wave detector. We plan to achive the improvement in the measurement accuracy by including into the scheme the machine learning algorithms capable to compensate the imprecision in the alignment of the optical

elements.

QUANTUM CRYPTOGRAPHY

The feasibility of the secure information transmission between the legitimate parties has been one of the central civilizational questions for millenia. Despite timeless concern, none of the subterfuge for protecting valuable data developed through centuries could withstand the rigorous mathematical criteria of secrecy: one could never guarantee that the data never comes out.

In the middle of the 20th century there has been established the set of conditions ensuring the absolute secrecy of communication:

1. the cryptographic key ciphering the secret message has to be completely random;
2. the key's length has to correspond to the length of the secret message;
3. the key has to be used only once.

These criteria pose a quest of finding a way for distributing random bit sequences privately among the legitimate parties each time before their communication takes place. This problem can be solved with quantum cryptography utilizing fundamental quantum principles which do not have analogues in the classical world [31, 32, 33].

The great expectations are placed on quantum cryptography also because it offers tools for protecting against the quantum threat – the possibility of breaking classical cryptographic protocols with quantum computers. In 1994, Peter Shor [34] proposed a quantum algorithm enabling one to rapidly factorize large numbers. This discovery immediately impared the security of the most widely used cryptosystem RSA [35] which is predicated upon the presumption that one cannot perform such factorization within a reasonable time. Therefore, with the emergence of a large-scale quantum computer, much of the classical cryptography will collapse.

Quantum key distribution (QKD) protocols offer the highest level of security and confidentiality although to this date, their practical implementations are still not ideal. A common quantum protocol for distributing a secret key between two parties consists of two stages: (i) quantum communication and (ii) classical post-processing. During the first stage the sender generates a random bit sequence and encodes it in quantum states which are then measured by the receiver. On the second stage, using the classical communication channel the authorised parties analyse the correlation between the sent and received data and perform additional measures to get rid of the invalid bits and eradicate information possibly intercepted by the eavesdropper. Due to the fact that quantum mechanics forbid perfect cloning of quantum states, the eavesdropper can only obtain partial information about the sent sequence and with that would disturb the quantum state.

On practice, the QKD realisations are typically characterised by a trade-off between the secret key generation speed and security: the practical QKD devices allow for the reasonable speeds but are susceptible to the external eavesdropper attacks; on the contrary, the device independent QKD schemes [36] ruling out the possibility of meddling into the key exchange are marked by small speeds. Another major trade-off is between the key generation speed and transmission distance. The development of the long-distance high-speed QKD devices above everything else requires reliable techniques for repeating quantum signals [37, 38, 39]. In the absence of such techniques, the best results are promised by the QKD protocols based on Gaussian states [40] and continuous variable states [41].

Despite the existing stumbling blocks, posed mainly by the early technological stage of the industry, Terra Quantum has achieved a significant progress towards delivering reliable commercial long-distance QKD solutions which will be both secure and efficient. Several other companies, among which are Qasky and Toshiba, have already developed commercial QKD systems which are being integrated in our daily life. Importantly, QKD is implemented in China's financial and governmental sectors [42, 43], and the Chinese quantum network covers more than 2000 km. Other countries, including the U.K. [44] and U.S., are launching their own quantum networks as well.

RANDOM NUMBER GENERATION

The cryptographic protocols like many other algorithms require large random information. Current random number generators (RNG) fall into two categories [45]: those which use deterministic mathematical functions to generate numbers computationally, and those which generate numbers based on physical measurements. The first type of RNG

produces the so-called pseudo-random numbers – although these numbers have random properties, their distribution is completely deterministic and can repeat and be repeated. The second type measures classical physical quantities which deviate randomly (e.g., temperature) and translates them into random numerical data. It appears that the second type of RNG is better as it exploits the true randomness of nature; however, this randomness has its own problems. First, there may be correlation between the measured data: for instance, two values of temperature measured at different times may be not fully independent of each other along with the corresponding random numbers. Second, the measured physical quantity can be deliberately manipulated by a perpetrator, which jeopardizes the secrecy of the random data.

Quantum technology opens route the true quantum randomness completely unpredictable and independent from environmental factors. Unlike the classical phenomena, the quantum events are associated with the quantum probabilities which are fundamentally different from the statistical ones. Terra Quantum is developing commercially available quantum RNG which will be predicated upon the single photon measurement. The quantum RNG will also be available online for the use of general public.

MRI SCANNER (ALGORITHMIC COOLING)

Nuclear magnetic resonance (NMR) effect describes the resonant absorption and emission of photons by nuclei in a strong constant magnetic field under the influence of another weak oscillating field [46]. The application domain of NMR spans the studies of porous media in the petroleum industry, the content analysis of the biological substances, the studies of polymers' properties in chemistry, and the magnetic resonance imaging (MRI) in medicine.

NMR provides the ground for realizing complex quantum procedures which may greatly enhance the current analytical methods. Among such procedures is the algorithmic cooling (also known as quantum algorithmic magnetic polarization transfer) – a novel approach enabling one to decrease the entropy of a spin system and cool it to extremely low temperatures [47]. This approach goes far beyond other existing spin-cooling techniques and opens rout for the unprecedentedly sensitive spectroscopy. Terra Quantum aims to bring algorithmic cooling to medicine by devising a high-sensitive geteronuclear MRI scanner. We expect that among all other things the device will enable imaging of organs which are hardly visible on the regular MRI scanners, particularly bones and lungs.

ACKNOWLEDGMENTS

This work is supported by the Government of the Russian Federation (Agreement 05.Y09.21.0018) and by Terra Quantum AG.

REFERENCES

1. QMWare, "The first global quantum cloud, https://qm-ware.com/,".
2. H. Neven, V. S. Denchev, G. Rose, and W. Macready, "QBoost: Large scale classifier training with adiabatic quantum optimization," in *ACML* (2012).
3. P. Rebentrost, M. Mohseni, and S. Lloyd, "Quantum support vector machine for big data classification," Phys. Rev. Lett. **113**, 130503 (2014).
4. V. Dunjko and H. J. Briegel, "Machine learning artificial intelligence in the quantum domain: a review of recent progress," Reports on progress in physics. Physical Society (Great Britain) **81** (2018), doi:10.1088/1361-6633/aab406.
5. J. R. McClean, M. P. Harrigan, M. Mohseni, N. C. Rubin, Z. Jiang, S. Boixo, V. N. Smelyanskiy, R. Babbush, and H. Neven, "Low depth mechanisms for quantum optimization," arXiv:2008.08615 (2020), arXiv:arXiv:2008.08615.
6. A. Peruzzo, J. McClean, P. Shadbolt, M.-H. Yung, X.-Q. Zhou, P. J. Love, A. Aspuru-Guzik, and J. L. O'Brien, "A variational eigenvalue solver on a photonic quantum processor," Nature Communications **5** (2014), 10.1038/ncomms5213.
7. E. Farhi and H. Neven, "Classification with quantum neural networks on near term processors," arXiv:1802.06002 (2018), arXiv:arXiv:1802.06002.
8. V. Havlíček, A. D. Córcoles, K. Temme, A. W. Harrow, A. Kandala, J. M. Chow, and J. M. Gambetta, "Supervised learning with quantum-enhanced feature spaces," Nature **567**, 209–212 (2019).
9. Q. V. Le, M. Ranzato, R. Monga, M. Devin, K. Chen, G. S. Corrado, J. Dean, and A. Y. Ng, "Building high-level features using large scale unsupervised learning," ICML (2012).
10. T. Elo, T. S. Abhilash, M. R. Perelshtein, I. Lilja, E. V. Korostylev, and P. J. Hakonen, "Broadband lumped-element Josephson parametric amplifier with single-step lithography," Applied Physics Letters **114**, 152601 (2019).
11. E. Magesan, J. M. Gambetta, A. D. Córcoles, and J. M. Chow, "Machine learning for discriminating quantum measurement trajectories and improving readout," Phys. Rev. Lett. **114**, 200501 (2015).

12. C. E. Granade, C. Ferrie, N. Wiebe, and D. G. Cory, "Robust online hamiltonian learning," New Journal of Physics **14**, 103013 (2012).
13. M. Krenn, M. Malik, R. Fickler, R. Lapkiewicz, and A. Zeilinger, "Automated search for new quantum experiments," Phys. Rev. Lett. **116**, 090405 (2016).
14. A. A. Melnikov, H. P. Nautrup, M. Krenn, V. Dunjko, M. Tiersch, A. Zeilinger, and H. J. Briegel, "Active learning machine learns to create new quantum experiments," Proceedings of the National Academy of Sciences **115**, 1221–1226 (2018).
15. S. Lloyd, "Enhanced sensitivity of photodetection via quantum illumination," Science **321**, 1463–1465 (2008).
16. J. C. Matthews, X.-Q. Zhou, H. Cable, P. J. Shadbolt, D. J. Saunders, G. A. Durkin, G. J. Pryde, and J. L. O'Brien, "Towards practical quantum metrology with photon counting," npj Quantum Information **2** (2016), 10.1038/npjqi.2016.23.
17. S. Danilin, A. V. Lebedev, A. Vepsäläinen, G. B. Lesovik, G. Blatter, and G. S. Paraoanu, "Quantum-enhanced magnetometry by phase estimation algorithms with a single artificial atom," npj Quantum Information **4**, 29 (2018).
18. A. Y. Kitaev, "Quantum measurements and the Abelian stabilizer problem," arXiv: quant-ph/9511026 (1995), arXiv:quant-ph/9511026 [quant-ph].
19. R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, "Quantum algorithms revisited," Proc. R. Soc. Lond. A. **454**, 339–354 (1998).
20. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, 2010).
21. J. Koch, T. M. Yu, J. Gambetta, A. A. Houck, D. I. Schuster, J. Majer, A. Blais, M. H. Devoret, S. M. Girvin, and R. J. Schoelkopf, "Charge-insensitive qubit design derived from the Cooper pair box," Phys. Rev. A **76**, 042319 (2007).
22. E. Il'ichev and Y. S. Greenberg, "Flux qubit as a sensor of magnetic flux," EPL **77**, 58005 (2007).
23. M. Bal, C. Deng, J.-L. Orgiazzi, F. R. Ong, and A. Lupascu, "Ultrasensitive magnetic field detection using a single artificial atom," Nature Communications **3**, 1324 (2012).
24. W. Wang, Y. Wu, Y. Ma, W. Cai, L. Hu, X. Mu, Y. Xu, Z.-J. Chen, H. Wang, Y. P. Song, H. Yuan, C.-L. Zou, L.-M. Duan, and L. Sun, "Heisenberg-limited single-mode quantum metrology in a superconducting circuit," Nature Communications **10**, 4382 (2019).
25. A. R. Shlyakhov, V. V. Zemlyanov, M. V. Suslov, A. V. Lebedev, G. S. Paraoanu, G. B. Lesovik, and G. Blatter, "Quantum metrology with a transmon qutrit," Phys. Rev. A **97**, 022115 (2018).
26. E. Knill, R. Laflamme, and G. J. Milburn, "A scheme for efficient quantum computation with linear optics," Nature **409**, 46–52 (2001).
27. J. P. Dowling and K. P. Seshadreesan, "Quantum optical technologies for metrology, sensing, and imaging," J. Lightwave Technol. **33**, 2359–2370 (2015).
28. J. Carolan, C. Harrold, C. Sparrow, E. Martin-Lopez, N. J. Russell, J. W. Silverstone, P. J. Shadbolt, N. Matsuda, M. Oguma, M. Itoh, G. D. Marshall, M. G. Thompson, J. C. F. Matthews, T. Hashimoto, J. L. O'Brien, and A. Laing, "Universal linear optics," Science **349**, 711–716 (2015).
29. S.-H. Tan and P. P. Rohde, "The resurgence of the linear optics quantum interferometer — recent advances applications," Reviews in Physics **4**, 100030 (2019).
30. V. V. Zemlyanov, N. S. Kirsanov, M. R. Perelshtein, D. I. Lykov, O. V. Misochko, M. V. Lebedev, V. M. Vinokur, and G. B. Lesovik, "Phase estimation algorithm for the multibeam optical metrology," Scientific Reports **10**, 8715 (2020).
31. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145–195 (2002).
32. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys. **81**, 1301–1350 (2009).
33. E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," npj Quantum Information **2**, 16025 (2016).
34. P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM Journal on Computing **26**, 1484–1509 (1997), https://doi.org/10.1137/S0097539795293172.
35. R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM **21**, 120–126 (1978).
36. J. Barrett, L. Hardy, and A. Kent, "No signaling and quantum key distribution," Phys. Rev. Lett. **95**, 010503 (2005).
37. H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication," Phys. Rev. Lett. **81**, 5932–5935 (1998).
38. W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, "Quantum repeaters based on entanglement purification," Phys. Rev. A **59**, 169–181 (1999).
39. L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, "Long-distance quantum communication with atomic ensembles and linear optics," Nature **414**, 413–418 (2001).
40. C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," Rev. Mod. Phys. **84**, 621–669 (2012).
41. S. L. Braunstein and P. van Loock, "Quantum information with continuous variables," Rev. Mod. Phys. **77**, 513–577 (2005).
42. T.-Y. Chen, H. Liang, Y. Liu, W.-Q. Cai, L. Ju, W.-Y. Liu, J. Wang, H. Yin, K. Chen, Z.-B. Chen, C.-Z. Peng, and J.-W. Pan, "Field test of a practical secure communication network with decoy-state quantum cryptography," Opt. Express **17**, 6540–6549 (2009).
43. T.-Y. Chen, J. Wang, H. Liang, W.-Y. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, W.-Q. Cai, L. Ju, L.-K. Chen, L.-J. Wang, Y. Gao, K. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, "Metropolitan all-pass and inter-city quantum communication network," Opt. Express **18**, 27217–27225 (2010).
44. J. F. Dynes, A. Wonfor, W. W.-S. Tam, A. W. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. L. Yuan, A. R. Dixon, J. Cho, Y. Tanizawa, J.-P. Elbers, H. Greißer, I. H. White, R. V. Penty, and A. J. Shields, "Cambridge quantum network," npj Quantum Information **5**, 101 (2019).
45. J. von Neumann, "Various techniques used in connection with random digits," in *Monte Carlo Method*, National Bureau of Standards Applied Mathematics Series, Vol. 12, edited by A. S. Householder, G. E. Forsythe, and H. H. Germond (US Government Printing Office, Washington, DC, 1951) Chap. 13, pp. 36–38.
46. I. I. Rabi, J. R. Zacharias, S. Millman, and P. Kusch, "A new method of measuring nuclear magnetic moment," Phys. Rev. **53**, 318–318 (1938).
47. D. K. Park, N. A. Rodriguez-Briones, G. Feng, R. Rahimi, J. Baugh, and R. Laflamme, "Heat bath algorithmic cooling with spins: Review and prospects," in *Electron Spin Resonance (ESR) Based Quantum Computing*, edited by T. Takui, L. Berliner, and G. Hanson (Springer New York, New York, NY, 2016) pp. 227–255.