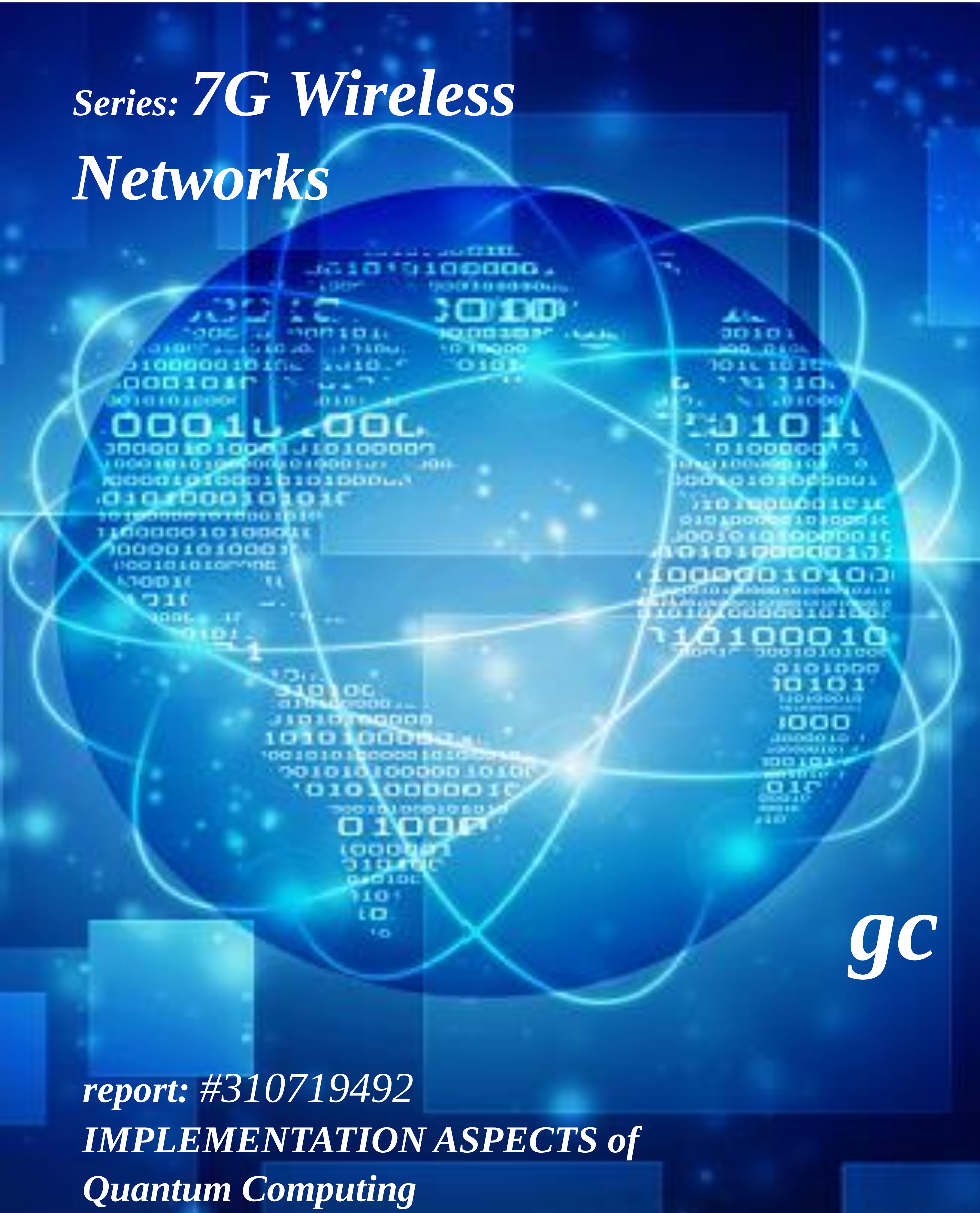

Series: *7G Wireless Networks*

gc

report: #310719492

IMPLEMENTATION ASPECTS of Quantum Computing

series: ***7G Wireless Networks***

report:310719492 ***IMPLEMENTATION ASPECTS of Quantum Computing***

by Savo Glisic
Worcester Polytechnic Institute, Massachusetts

GC Institute for Networking Sciences

Preface: The research and practical results on Quantum computers in the recent years have given a major setback to classical and widely used cryptography schemes such as RSA (Rivest-Shamir-Adleman) Algorithm and ECC (Elliptic Curve Cryptography). RSA and ECC depend on integer factorization problem and discrete logarithm problem respectively, which can be easily solved by Quantum Computers of sufficiently large size running the infamous Shor's Algorithm. Therefore, cryptography schemes which are difficult to solve in both traditional as well as Quantum Computers need to be evaluated. This series of reports provides a detailed survey on Post-Quantum Cryptography schemes and emphasizes on their applicability to provide security in constrained devices. A comprehensive insight is provided into the schemes which could possibly replace RSA and ECC for security in constrained devices.

While post-quantum cryptography is an effort to develop novel classical cryptosystems which are robust to factorization and other quantum algorithms, which is certainly one option, this does not completely solve the problem. The point is that there may be undiscovered quantum algorithms (or undiscovered classical ones) that might easily break the security of the new cryptosystems. In other words, postquantum cryptography is likely to offer only a partial and temporary solution to the problem. By contrast, quantum key distribution (QKD), discussed also in this series, offers the ultimate solution: restoring security and confidentiality by resorting to unbreakable principles of nature, such as the uncertainty principle or the monogamy of entanglement.

Even though QKD offers the ultimate solution to the security problem, its ideal implementation is hard to implement in practice and there are a number of open problems to be addressed. On one side, fully-device independent QKD protocols provide the highest level of quantum security, but they are quite demanding to realize and are characterized by extremely low secret key rates. On the other hand, more practical QKD protocols assume some level of trust in their devices, an assumption that allows them to achieve reasonable rates, but this also opens the possibility of dangerous side-channel attacks.

Besides a trade-off between security and rate, there is also another important one which is between rate and distance. Today, we know that there is a fundamental limit which restricts any point to point implementation of QKD. Given a lossy link with transmissivity η, two parties cannot distribute more than the secret key capacity of the channel, which is $-log_2(1-\eta)$, i.e., a scaling of 1.44η secret bits per channel use at long distance. Ideal implementations of QKD protocols based on continuous-variable systems and Gaussian states may approach this capacity , while those based on discrete variables falls below by additional factors. To overcome this limit and enable long-distance high-rate implementations of QKD, we need the develop quantum repeaters and quantum networks . In this way, we may achieve better long-distance scaling and further boost the rates by resorting to more complex routing strategies. The study of quantum repeaters and secure QKD networks is one of the hottest topics today which is also covered in this series. The series aims at providing an overview of the most important and most recent advances in the field of quantum cryptography, both theoretically and experimentally.

In near term, we expect that quantum security and QKD will be competing with so called post quantum security solutions and for this reason in a separate report of this series we discuss in details pros and cons of each technology. ***Design solutions and quantum physics are covered in this report****.*

When it comes to using the book for undergrade and postgraduate courses we incorporate a number of DESIGN EXAMPLES in each report to replace the classical concept of using "problems and solutions" addendums at the end of the chapters/book. This enables using more sophisticated assignments for the teamwork of the students. Our students have shown great enthusiasm for such approach.

In addition to universities the professionals in research, industry and regulatory institutions should benefit from the comprehensive coverage of different report of the series.

Author, March 2022 *Amherst, Massachusetts,* https://www.youtube.com/watch?v=u1XXjWr5frE

Ch1 INTRODUCTION

1.1 Structure of the book

Given the above objective, we present the overall material of the book within 5 chapters and in what follows we briefly summarize the content of these chapters.

Ch 2 QUANTUM COMPUTING GATES LIBRARIES The circuit model of a computer is an abstraction of the computing process and is widely used in the design and construction of practical computing hardware. In the circuit model, any computation is regarded as being equivalent to the action of a circuit built out of a handful of different types of Boolean logic gates acting on some binary (i.e., bit string) input. Each logic gate transforms its input bits into one or more output bits in some deterministic fashion according to the definition of the gate. By composing the gates in a graph such that the outputs from earlier gates feed into the inputs of later gates, it can be proven that any feasible computation can be performed. Here we will talk about the types of logic gates used within circuits and how the notions of logic gates need to be modified in the quantum context.

Ch 3 Q MEMORIES Quantum memories are a fundamental of any global-scale quantum Internet. Although quantum repeaters can be realized without the necessity of quantum memories, these units, in fact, are required for guaranteeing an optimal performance in any high-performance quantum networking scenario. Therefore, the utilization of quantum memories still represents a fundamental problem in the quantum Internet, since the near-term quantum devices (such as quantum repeaters) and gate-model quantum computers have to store the quantum states in their local quantum memories . The main problem here is the efficient readout of the stored quantum systems and the low retrieval efficiency of these systems from the quantum registers of the quantum memory. Currently, no general solution to this problem is available, since the quantum register evolves the stored quantum systems via an unknown operation, and the input quantum system is also unknown, in a general scenario. The optimization of the readout procedure is therefore a hard and complex problem. Several physical implementations have been developed in the last few years . However, these experimental realizations have several drawbacks, in general because the output signal-to-noise ratio (SNR) values are still not satisfactory for the construction of a powerful, global-scale quantum communication network. As another important application field in quantum communication, the methods of quantum secure direct communication - also require quantum memory.

Here, we discuss a specific quantum memory called high-retrieval-efficiency (HRE) quantum memory for near-term quantum devices. An HRE quantum memory unit integrates local unitary operations on its hardware level for the optimization of the readout procedure.
An HRE quantum memory unit utilizes the advanced techniques of quantum machine learning to achieve a significant improvement in the retrieval efficiency.

Ch 4 IMPLEMENTATION EXAMPLES OF cv QKD In the set of general assumptions for the system implementation we allow eavesdropper (node E) to have full access to the quantum channel which she is free to control and manipulate. She can monitor the public channel but cannot intervene in the conversation between node A and node B which introduces the important requirement of an authenticated channel. For her eavesdropping attack, E is allowed to prepare arbitrary ancillary states that she gets to interact with the transmitted signal states and subsequently performs measurements on. She might be in possession of a quantum memory which allows her to store her states and perform her measurement at a later time according to what she learned during the classical post-processing. The actual degree of information-theoretic security of a given QKD protocol depends strongly on the assumed technological capabilities a potential eavesdropper might have. Classified by her powers, we distinguish three different types of eavesdropping attacks (i.e. attempts to obtain information on the secret key) that are typically considered in security proofs: Individual attack, Collective attack, Coherent attack. A comprehensive analysis of the system behavior within the framework of these assumptions id presented. Here, we also present in more details several QKD implementations of specific interest for 6/7G networks. As the first step we investigate the performance of QKD over THz band since this band is of interest already for 6G and will continue to be of interest for 7G as well. A network architecture of hybrid trusted/untrusted relay based QKD over optical backbone networks is also described along with the description of the structure of the nodes in such network. The chapter is wrapped up wit a comprehensive discussion on receiver design for QKD.

Ch 5 qubit PHYSICS Over the past two decades, rapid developments in the science and engineering of quantum systems have advanced the frontier in quantum computation, from the realm of scientific explorations on single isolated quantum systems toward the creation and manipulation of multi ‑ qubit processors [11-12] . In particular, the requirements imposed by larger quantum processors have shifted mindset within the community, from solely scientific discovery to the development of new, foundational engineering abstractions associated with the design, control, and readout of multiqubit quantum systems. The result is the emergence of a new discipline termed quantum engineering, which serves to bridge the basic sciences, mathematics, and computer science with fields generally associated with traditional engineering.

One prominent platform for constructing a multi ‑ qubit quantum processor involves superconducting qubits, in which information is stored in the quantum degrees of freedom of nano fabricated, anharmonic oscillators constructed from superconducting circuit elements [1-10]. Alternative platforms, e.g. electron spins in silicon [13-18] and quantum dots [19 − 22], trapped ions [23 − 27] , ultracold atoms [28 − 31], nitrogen ‑ vacancies in diamonds [32 − 33], and polarized photons [34 − 37], have been also developed. In this chapter we review main characteristics of these groups of technologies.

REFERENCES

[1] M. H. devoret and J. M. Martinis , “Implementing qubits with superconducting integrated circuits,” Quantum Information Processing 3, 63-103 (1004).

[2] J. Q. You and F. Nori, “Superconducting circuits and quantum information,” Physics Today 58, 42-47 (1005).

[3] R. J. Schoelkopf and S. M. Girvin, “Wiring up quantum systems,” Nature 451, 664 (1008).

[4] J. Clarke and F. K. Wilhelm, “Superconducting quantum bits.” Nature 453, 1031-42 (1008).

[5] S. M. Girvin, Circuit QED : Superconducting Qubits Coupled to Microwave Photons (Oxford University Press, Oxford, England, 1009).

[6] J. Q. You and F. Nori, “Atomic physics and quantum optics using superconducting circuits,” Nature 474, 589 (1011).

[7] W. D. Oliver and P. B. Welander, “Materials in superconducting quantum bits,” MRS Bulletin 38, 86-825 (103).

[8] J. M. Gambetta, J. M. Chow, and M. Steffen, “Building logical qubits in a superconducting quantum computing system,” npj Quantum Information 3, 2 (107).

[9] G. Wendin, “Quantum information processing with superconducting circuits: a review,” Reports on Progress in Physics 80, 106001 (107).

[10] X. Gu, A. F. Kockum, A. Miranowicz, Y. x Liu, and F. Nori, “Microwave photonics with superconducting quantum circuits,” Physics Reports 78-79, 1—102 (107).

[11] C. Monroe and J. Kim, “Scaling the ion trap quantum processor,” Science 339, 164 ‑ 169 (103).

[12] H. Bernien , S. Schwartz , A. Keesling, H. Levine, A. Omran, H. Pichler , S. Choi , A. S. Zibrov , M. Endres , M. Greiner, V. Vuletić, and M. D. Lukin, “Probing many ‑ body dynamics on a 51 ‑ atom quantum simulator,” Nature 551, 579 (107).

[13] D. Loss and D. P. DiVincenzo , “Quantum computation with quantum dots,” Phys. Rev. A 57, 10 ‑ 26 (998).

[14] B. E. Kane, “A silicon ‑ based nuclear spin quantum computer,” Nature 393, 33 (998).

[15] R. Vrijen, E. Yablonovitch, K. Wang, H. W. Jiang, A. Balandin, V. Roychowdhury, T. Mor, and D. DiVincenzo, “ Electronspin ‑ resonance transistors for quantum computing in silicongermanium heterostructures,” Phys. Rev. A 62, 02306 (1000).

[16] R. de Sousa, J. D. Delgado, and S. Das Sarma, “Silicon quantum computation based on magnetic dipolar coupling, ” Phys. Rev. A 70, 052304 (1004).

[17] L. C. L. Hollenberg, A. D. Greentree, A. G. Fowler, and C. J. Wellard, “Two ‑ dimensional architectures for donor ‑ based quantum computing,” Phys. Rev. B74, 045311 (1006).

[18] A. Morello, J. J. Pla, F. A. Zwanenburg, K. W. Chan, et al, “Singleshot readout of an electron spin in silicon,” Nature 467, 687 (1010).

[19] A. Imamoglu, D. D. Awschalom, G. Burkard, D. P. DiVincenzo, D. Loss , M. Sherwin , and A. Small “Quantum information processing using quantum dot spins and cavity QED,” Phys. Rev. Lett. 83, 4104 ‑ 4107 (999).

[20] J. R. Petta, A. C. Johnson, J. M. Taylor, E. A. Laird, A. Yacoby, M. D. Lukin, C. M. Marcus, M. P. Hanson, and A. C. Gossard, “Coherent manipulation of coupled electron spins in semiconductor quantum dots,” Science 309, 280 ‐284 (1005).

[21] D. Englund, D. Fattal, E. Waks, G. Solomon, B. Zhang, T. Nakaoka , Y. Arakawa , Y. Yamamoto , and J. Vučković, “Controlling the spontaneous emission rate of single quantum dots in a two ‐dimensional photonic crystal,” Phys. Rev. Lett. 95, 03904 (1005).

[22] R. Hanson, L. P. Kouwenhoven, J. R. Petta, S. Tarucha, and L. M. K. Vandersypen, “Spins in few ‐electron quantum dots,” Rev. Mod. Phys. 79, 27 ‐265 (1007).

[23] J. I. Cirac and P. Zoller , “Quantum computations with cold trapped ions,” Phys. Rev. Lett. 74, 4091 ‐4094 (995).

[24] D. Leibfried, R. Blatt, C. Monroe, and D. Wineland, “Quantum dynamics of single trapped ions,” Rev. Mod. Phys. 75, 281 ‐324 (1003).

[25] R. Blatt and D. Wineland, “Entangled states of trapped atomic ions,” Nature 453, 1008 (1008).

[26] H. Häffner, C. Roos, and R. Blatt, “Quantum computing with trapped ions,” Physics Reports 469, 55–103 (1008).

[27] R. Blatt and C. F. Roos, “Quantum simulations with trapped ions,” Nature Physics 8, 277 (102).

[28] D. Jaksch and P. Zoller, “The cold atom hubbard toolbox,” Annals of Physics 35, 52–79 (1005), special Issue.

[29] M. Lewenstein , A. Sanpera, V. Ahufinger, B. Damski, A. Sen(De), and U. Sen, “Ultracold atomic gases in optical lattices: mimicking condensed matter physics and beyond,” Advances in Physics 56, 243 ‐379 (1007).

[30] I. Bloch, J. Dalibard, and W. Zwerger, “Many ‐body physics with ultracold gases,” Rev. Mod. Phys. 80, 885 ‐964 (1008).

[31] C. Gross and I. Bloch, “Quantum simulations with ultracold atoms in optical lattices,” Science 357, 995 ‐1001 (107).

[32] R. Hanson , O. Gywat, and D. D. Awschalom, “Roomtemperature manipulation and decoherence of a single spin in diamond,” Phys. Rev. B74, 6103 (1006).

[33] M. V. G. Dutt , L. Childress , L. Jiang, E. Togan, J. Maze, F. Jelezko, A. S. Zibrov, P. R. Hemmer, and M. D. Lukin, “Quantum register based on individual electronic and nuclear spin qubits in diamond,” Science 36, 32 ‐36 (1007).

[34] E. Knill, R. Laflamme, and G. J. Milburn, “A scheme for efficient quantum computation with linear optics,” Nature 409, 46 (1001).

[35] T. B. Pittman, B. C. Jacobs, and J. D. Franson, “Probabilistic quantum logic operations using polarizing beam splitters,” Phys. Rev. A 64, 062311 (1001).

[36] J. D. Franson, M. M. Donegan, M. J. Fitch, B. C. Jacobs, and T. B. Pittman, “High ‐fidelity quantum logic operations using linear optical elements,” Phys. Rev. Lett. 89, 37901 (1002).

[37] T. B. Pittman, M. J. Fitch, B. C. Jacobs, and J. D. Franson, “Experimental controlled ‐not logic gate for single photons in the coincidence basis,” Phys. Rev. A 68, 03236 (1003).

[38] C. Belacel, Y. Todorov, S. Barbieri, D. Gacemi, I. Favero, and C. Sirtori,“Optomechanical terahertz detection with single meta-atom resonator,”Nature Commun., vol. 8, Nov. 107, Art. no. 578.

[39] S. Glisic and B. Lorenzo, Artificial Intelligence and Quantum Computing for Advanced Wireless Networks, John Wiley, 2022

[40] S. L. Braunstein and P. van Loock, “Quantum information with continuous variables,” Rev. Mod. Phys., vol. 77, no. 2, p. 53, 1005.

The research and practical results on Quantum computers in the recent years have given a major setback to classical and widely used cryptography schemes such as RSA (Rivest-Shamir-Adleman) Algorithm and ECC (Elliptic Curve Cryptography). RSA and ECC depend on integer factorization problem and discrete logarithm problem respectively, which can be easily solved by Quantum Computers of sufficiently large size running the infamous Shor's Algorithm. Therefore, cryptography schemes which are difficult to solve in both traditional as well as Quantum Computers need to be evaluated. This series of reports provides a detailed survey on Post-Quantum Cryptography schemes and emphasizes on their applicability to provide security in constrained devices. A comprehensive insight is provided into the schemes which could possibly replace RSA and ECC for security in constrained devices.

While post-quantum cryptography is an effort to develop novel classical cryptosystems which are robust to factorization and other quantum algorithms, which is certainly one option, this does not completely solve the problem. The point is that there may be undiscovered quantum algorithms (or undiscovered classical ones) that might easily break the security of the new cryptosystems. In other words, postquantum cryptography is likely to offer only a partial and temporary solution to the problem. By contrast, quantum key distribution (QKD), discussed also in this series, offers the ultimate solution: restoring security and confidentiality by resorting to unbreakable principles of nature, such as the uncertainty principle or the monogamy of entanglement.

Even though QKD offers the ultimate solution to the security problem, its ideal implementation is hard to implement in practice and there are a number of open problems to be addressed. On one side, fully-device independent QKD protocols provide the highest level of quantum security, but they are quite demanding to realize and are characterized by extremely low secret key rates. On the other hand, more practical QKD protocols assume some level of trust in their devices, an assumption that allows them to achieve reasonable rates, but this also opens the possibility of dangerous side-channel attacks.

Besides a trade-off between security and rate, there is also another important one which is between rate and distance. Today, we know that there is a fundamental limit which restricts any point to point implementation of QKD. Given a lossy link with transmissivity η, two parties cannot distribute more than the secret key capacity of the channel, which is $-log_2(1-\eta)$, i.e., a scaling of 1.44η secret bits per channel use at long distance. Ideal implementations of QKD protocols based on continuous-variable systems and Gaussian states may approach this capacity , while those based on discrete variables falls below by additional factors. To overcome this limit and enable long-distance high-rate implementations of QKD, we need the develop quantum repeaters and quantum networks . In this way, we may achieve better long-distance scaling and further boost the rates by resorting to more complex routing strategies. The study of quantum repeaters and secure QKD networks is one of the hottest topics today which is also covered in this series. The series aims at providing an overview of the most important and most recent advances in the field of quantum cryptography, both theoretically and experimentally.

In near term, we expect that quantum security and QKD will be competing with so called post quantum security solutions and for this reason in a separate report of this series we discuss in details pros and cons of each technology. ***Design solutions and quantum physics are covered in this report****.*

When it comes to using the book for undergrade and postgraduate courses we incorporate a number of DESIGN EXAMPLES in each report to replace the classical concept of using "problems and solutions" addendums at the end of the chapters/book. This enables using more sophisticated assignments for the teamwork of the students. Our students have shown great enthusiasm for such approach.

In addition to universities the professionals in research, industry and regulatory institutions should benefit from the comprehensive coverage of different report of the series.