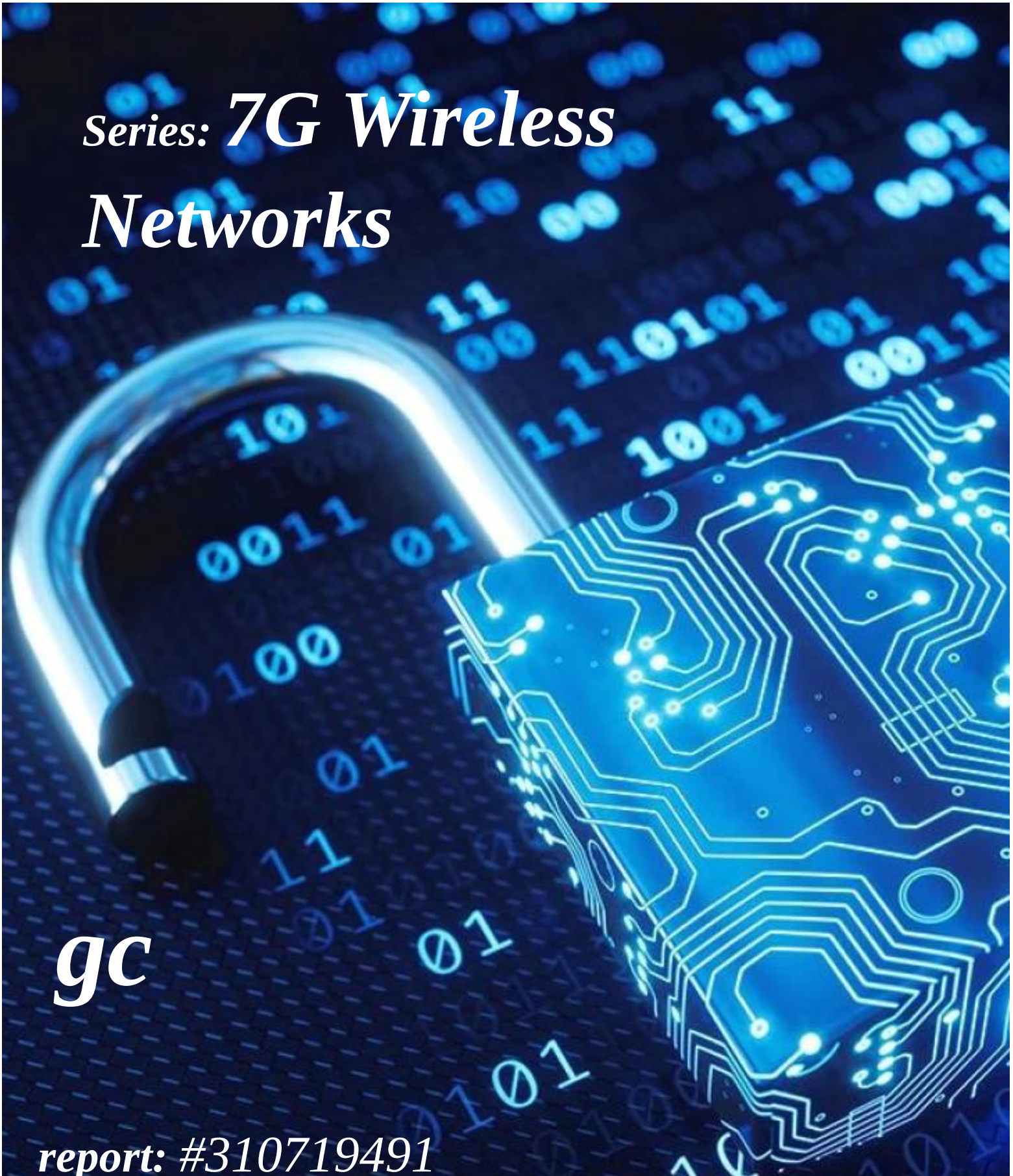

Series: ***7G Wireless Networks***

gc

report: *#310719491*

Continuous Variable QUANTUM KEY DISTRIBUTION over Wireless NETWORKS

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

report: #310719491 ***Continuous Variable QUANTUM KEY DISTRIBUTION over WIRELESS NETWORKS***

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. The focus of this report is on QKD over wireless networks.

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 also included in another separate report of the series.

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 3 chapters and in what follows we briefly summarize the content of these chapters.

Ch 2 CV QUANTUM KEY DISTRIBUTION: One the most important results in the field of quantum information processing and communication is the ability to distribute secret keys between two parties with information-theoretic security, that is regardless of the capacities of a malevolent eavesdropper. Quantum key distribution (QKD) illustrates the power of encoding information on the quantum properties of light and has far-reaching implications in high-security applications. Today, quantum key distribution systems operate in real-world conditions and are commercially available. As with most quantum information protocols, quantum key distribution was first designed for qubits, the individual quanta of information. However, the use of quantum continuous variables for this task presents important advantages with respect to qubit-based protocols, from a practical point of view, since it allows for simple implementations that require only standard telecommunication technology. In this chapter, we describe the principle of continuous-variable quantum key distribution, focusing in particular on protocols based on coherent states. We discuss the security of these protocols and review the state-of-the-art in experimental implementations, including the results on sub optical (THz band) channels.

Ch 3 QKD OVER SUBOPTICAL BANDS: Towards Heterogenous Wireless & cv Quantum Networks

For the anticipated integration of wireless and quantum networks and enhancement of wireless network security, feasibility of QKD over suboptical bands is very important. In this chapter we summarize results in QKD over sub-optical bans including discussion on: cv QKD with Adaptive Multicarrier Quadrature Division Modulation, Multicarrier Quadrature Division Modulation, Adaptive Modulation Variance, Efficiency of AMQD Modulation, QKD over THz Band, TERAHERTZ QKD: System Model, System performance in the Extended Terahertz range, Derivation of the secret-key rates, Coherent Bidirectional Terahertz-Optical Converter, Implementation aspects, Quantum cryptography at wavelengths considerably longer than optical, Summary of analytical tools.

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. The focus of this report is on QKD over wireless networks.

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 also included in another separate report of the series.

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.