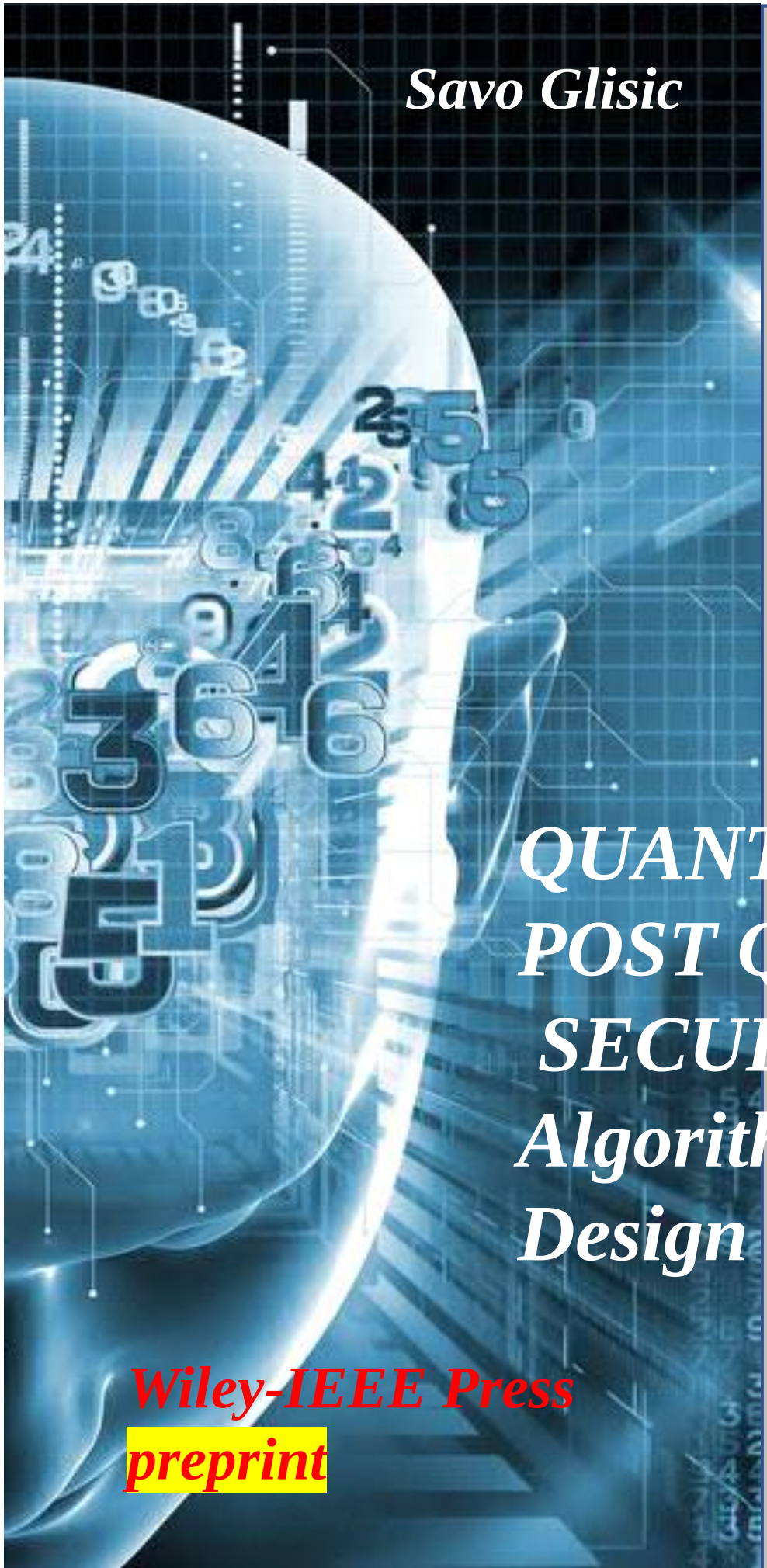

Savo Glisic

QUANTUM vs POST QUANTUM SECURITY: Algorithms and Design Technology

Wiley-IEEE Press

preprint

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 book 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 book, 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. In order 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 book. The book 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 here we discuss in details pros and cons of each technology. Design solutions and quantum physics are also included in the book.

When it comes to using the book for undergrade and postgraduate courses we incorporate a number of DESIGN EXAMPLES 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 the book.