Quantum Information and Computation, Vol. 7, No. 5&6 (2007) 571–572

BOOK REVIEW

on

PROTECTING INFORMATION: FROM CLASSICAL ERROR CORRECTION TO QUANTUM CRYPTOGRAPHY

by Susan Loepp and William Wootters

Cambridge University Press, 2006
Paperback $29.99 (304 pages) ISBN: 052153-476-3

Quantum information science promises not only new technologies but a new understanding of quantum mechanics. In the case of QKD both of these promises have been partially honoured. There are now a handful of companies selling QKD systems and an effort is underway to determine how to integrate QKD into the optical communication network . The security proofs of QKD have provided new insight into the subtle way in which the quantum world instantiates the principle of no superluminal signalling: a principle that possibly points to a deeper level of understanding of quantum mechanics. It is thus wonderful to see such a lucid and elegant introduction to the subject in *Protecting information: From classical error correction to quantum Cryptography*, by Susan Loepp and William Wooters (Cambridge University Press, 2006).

The first chapter is a simple introduction to Cryptography and contains concise explanations of classical ciphers, including a fascinating discussion of the Enigma cipher used by the German forces in the Second World War. The chapter goes on to discuss block ciphers, DES and public key cryptosystems. In each case the presentation is clear and uncluttered, with footnotes to direct readers to more detailed presentations. The chapter assumes no previous exposure to cryptosystems but very quickly takes the beginner through the basics.

Chapter 2 is an introduction to quantum mechanics that again assumes no previous exposure to the subject. The quantum theory can roughly be said to break down into two components: firstly, a probability amplitude calculus that enables one to compute the probability distributions for measurement results, once the probability amplitudes are given and, secondly, a number of methodologies (Schroedinger mechanics, quantum electrodynamics) that enables one to get the probability amplitudes in the first place. In this chapter the basic elements of the first component are well explained. The discussion is based on the physical example of photon polarisation. There is just enough detail to prepare someone with interests primarily in cryptography to grasp the later chapters. Very little physical background is required. Unfortunately, while this is economical, it does rather limit the level of understanding that could be achieved. For example, there is a possibility that an inattentive student might think that the polarisation vector of light and the two dimensional vector used to describe its quantum state, are the same thing. They are not: the former refers to the electric field vector, which lives in ordinary three dimensional physical space, while the latter is list of probability amplitudes and lives in Hilbert space. But as an introduction to the probability calculus, the

presentation is wonderful.

The third chapter gives an explanation of the Bennett-Brassard protocol for quantum key distribution, with a good explanation of how quantum mechanics ensures that an eavesdropper on the protocol can never remain undetected. It includes a rather brief discussion of the quantum no-cloning theorem and teleportation as they apply to qubits. The basic formalism of teleportation is explained but the discussion concludes very far short of the depth required to understand recent experiments. Again, footnotes direct the interested reader to other sources.

Here as elsewhere the discussion of QKD inevitably begins with Alice and Bob sending single photons to each other. Easy to say, but very hard to do! The curious interplay between the physics and the mathematics of QKD again becomes apparent the moment we ask for just a little bit more detail on what precisely we mean by sending a single photon. In fact all current commercial implementations of QKD are vulnerable precisely because of the flawed way in which they implement a single photon source. A true single photon source is a pulsed light source in which the probability of detecting one and only one photon per pulse is close to unity. This is a highly non-classical light source and a huge effort is being expended to develop such sources.

The discussion then reverts, in chapter 4, to classical matters while the authors explain the basics of error correcting codes. Starting from zero knowledge the student is led to a surprisingly high level of sophistication and at the end is rewarded with a delightful discussion of the Hat Problem. Chapter 5 returns to QKD to explain how error correction and privacy amplification can be used to dramatically improve the security of a QKD channel. Just enough of privacy amplification is explained to enable the beginner to get a good grasp on the subtle business of defeating an eavesdropper. As the authors hint at, just how subtle an eavesdropper can be depends on the technological capability for making quantum measurements on optical fields - a technology that hardly exists even in the physics lab - fortunately for QKD. The authors sign off on error correction with a relatively digestible discussion of Reed-Solomon codes in Chapter 7.

We now have great confidence that QKD is a secure way to transact private communication, although we have a long way to go in building the required technology to make it a reality. Even further from reality is the subject of the final chapter: quantum computing. The authors content themselves with a compact but comprehensible introduction to the basic concepts, including a detailed discussion of Shor's factoring algorithm: the discovery of which is largely responsible for the huge investment in experimental efforts in the field. The reason for this is that, as the authors explain, public key cryptosystems would be vulnerable to attack if a sufficiently large quantum computer was built. In fact that is not the fundamental reason why a large number of optimistic people take quantum computing seriously enough to try and build one: were it not for the discovery of quantum error correction quantum computing would have forever remained a footnote to quantum mechanics. This delightful book thus fittingly ends with a short coda on quantum error correction.

I highly recommend this book to all beginning students in quantum information – theorists and experimentalists alike. A major feature of the book is the set of extensive exercises, embedded in the text, to ease the path of a diligent student. The quality of the explanations and clarity of the writing will ensure that well-thumbed copies of this book will soon be found on many desks.

Gerard J. Milburn (milburn@physics.uq.edu.au)
The University of Queensland, St Lucia 4072 Australia