4th International Conference on Mathematical Modeling in Physical Sciences (IC-MSquare2015) IOP Publishing
Journal of Physics: Conference Series **633** (2015) 012029 doi:10.1088/1742-6596/633/1/012029

Post-quantum attacks on key distribution schemes in the presence of weakly stochastic sources

S W Al–Safi and C M Wilmott

Department of Physics and Mathematics, Nottingham Trent University, Clifton Campus, Nottingham NG11 8NS, UK

E-mail: sabri.alsafi@ntu.ac.uk, colin.wilmott@ntu.ac.uk

Abstract. It has been established that the security of quantum key distribution protocols can be severely compromised were one to permit an eavesdropper to possess a very limited knowledge of the random sources used between the communicating parties. While such knowledge should always be expected in realistic experimental conditions, the result itself opened a new line of research to fully account for real–world weak randomness threats to quantum cryptography. Here we expand of this novel idea by describing a key distribution scheme that is provably secure against general attacks by a post-quantum adversary. We then discuss possible security consequences for such schemes under the assumption of weak randomness.

1. Introduction

Considerable efforts have been advanced in recent years which have yielded good insights into the relative structure of quantum theory. These efforts have been important from the view of better understanding the quantum framework, but, interestingly, they have also provided speculative arguments regarding the existence and structure of physical theories which may well supersede quantum theory. These alternative physical theories have been formulated under a set of mathematically intuitive operational representations, and are referred to as general probabilistic theories. Within this class of general probabilistic theories, a possible alternative to quantum theory called *Boxworld* has emerged. That aspect of Boxworld which has identified itself from other general theories relates to the set of correlations it produces. While a defining feature of quantum theory has been the non–local correlations it produces, these being correlations that cannot be produced by any local hidden variable theory, Boxworld, on the other hand, generates non–signalling correlations that are beyond those admitted by quantum theory. These non–signalling correlations have extremely powerful features, and were first studied by Popescu and Rohrlich, and accordingly called *PR–boxes* (Popescu and Rohrlich 1994). Indeed, to understand the potential of Boxworld, and general probabilistic theories is to appreciate the significance of PR–boxes. Amongst others, PR–boxes offer a non-local resource that would render communication complexity a trivial task, and they can also be used to violate information casuality.

While Boxworld finds itself on the upside of advantage, the same certainly remains true for quantum theory. Examples abound, but in relation to security and cryptography, there are a number of pertinent results. Shor's quantum algorithm holds profound implications for the security of classical cryptography (Shor 1994), and, yet, despite this outstanding individual

result, the concept of cryptography has managed to evade redundancy as quantum theory comes equipped with its own style of cryptography called *quantum key distribution (QKD)*. QKD protocols enable pairs of communicating parties to produce shared random secret keys, which in turn, can be used to implement an unconditionally secure encryptions. Assuming the correctness of quantum theory, usual QKD protocols have been shown to be provably secure against eavesdropping attacks. Against the backdrop of general probabilistic theories, QKD has been found to be quite resilient. In particular, Barrett *et al.* (2005) have described a quantum key distribution scheme that is provably secure against arbitrary attacks by a post-quantum eavesdropper. In this post-quantum scenario, the eavesdropper is permitted to break the laws of quantum theory, but is limited solely by the impossibility of superluminal signalling. This is a remarkable result because, while the implication is that current QKD protocols may no longer be appropriate, Barrett *et al.* (2005) have, simultaneously, provided a revised quantum scheme that is secure against a non–signalling, post–quantum eavesdropper.

Quantum theory via key distribution has provided us with a provably secure way to communicate, but were quantum theory to ever fail, Barrett *et al.* (2005) have shown that we can rely on a quantum scheme that is secure against general attacks by a post-quantum eavesdropper. So, a big hurrah for QKD! Or, is it? Recent work by Bouda *et al.* (2012) examined QKD security issues arising when an adversary, aside from having full control of the various quantum and classical channels, has very limited access to the random sources employed by the communicating parties. They showed that with an increasing key length, only a negligible control of the randomness was necessary to render QKD insecure. This result illustrated that a vulnerability of quantum technology lies not with its science but in its practice of assuming perfectly uniform random processes. Indeed, both academia and industries specializing in commercial quantum technologies have blindly overlooked this fact by making assumptions that are fine in theory but not in practice. In this paper, we will outline an approach to examine the setup of a key distribution scheme robust against post-quantum attacks in light of results presented by Bouda *et al.* (2012). In section 2, we will outline some some basic facts relating to generalized probabilistic theories; in section 3, we present a quantum scheme based on Barrett *et al.*'s construction; and in section 4, we discuss various quantities relating to weak sources of randomness that may affect the real–world practical implementation of post-quantum cryptographic setups.

2. Preliminaries

2.1. Non-signalling constraints

We shall now motivate an operational setup for defining general probabilistic theories. As mentioned earlier, general probabilistic theories are compared and contrasted against the correlations they produce. These correlations are best described in terms of system probabilities that are ascribed to an outcome as a result of local measurements. Let $p(a, b|x, y)$ denote the probability of outcomes a and b given respective measurement choices, x and y. The value $p(a, b|x, y)$ respects the usual probability constraints. Thus, we have

$$0 \leq p(a, b|x, y) \leq 1 \tag{1}$$

for all measurement and outcome choices, and, for any fixed choice of local measurements,

$$\sum_{x,y} p(a, b|x, y) = 1. \tag{2}$$

We assume that correlations occur independently of the spatial separation between the systems, and demand that information cannot be communicated between the systems. This latter condition forces us to exclude those correlations that would permit the superluminal transmission

of information, and, instead, we ascribe to position that outcome probabilities, for any subset of systems, must not be affected by local measurement choices of other systems. In mathematical terms, we, therefore, require that:

$$p(a|x) = \sum_b p(a,b|x,y) \quad \forall y;$$
$$p(b|y) = \sum_a p(a,b|x,y) \quad \forall x. \tag{3}$$

We refer to this requirement as the non-signalling principle.

2.2. Generalized probabilistic theories

Post-quantum correlations are described in terms of a set of conditional probability distributions. However, it is often convenient to represent the associated generalized probabilistic theory by a real vector space $\mathbb{R}$ whereby states s and effects e are specified by vectors such that $\langle e, s\rangle$ defines the probability of the effect e occurring in the state s. Therefore, analogous to quantum theory, we can prepare the usual combination of states s_i with probabilities p_i in the mixed state $s = \sum_i p_i s_i$ with $p_i > 0$ and $\sum_i p_i = 1$. The set of allowed states is given by the convex state space $\mathcal{S} \subset \mathbb{R}$, for which the set of pure states are represented by the extremal points of $\mathcal{S}$.

Next, we correspond a measurement outcome to an effect. This is a function that maps every state to a probability in the interval [0,1], and is well–defined for probabilistic mixtures of states. Consequently, the set of allowed effects is the set of vectors $e_i \in \mathbb{R}$ such that $0 \leq \langle e_i, s\rangle \leq 1$ and $\sum_i \langle e_i, s\rangle = 1$ for all $s \in \mathcal{S}$. The unit effect u is the unique effect that corresponds to the measurement with only one outcome that is certain to occur; $\langle u, s\rangle = 1$ for all $s \in \mathcal{S}$. Finally, we shall make use of unnormalized states $\tilde{s} = \lambda s$, $\lambda \geq 0$, and note that the set of unnormalized states yields the positive cone $\mathcal{S}_+$.

By way of example, we can demonstrate the versatility of generalized probabilistic theories and recover both classical and quantum theories. In the case of classical theory, every pure state s_i corresponds to an effect e_i via $\langle e_i, s_j\rangle = \delta_{ij}$, and mixed state representations have a unique decomposition into pure states. The dimension of the associated system is given by the maximal number of linearly independent vector that form a basis, and the system itself is given by a simplex. In terms of quantum theory, states and effects are given as positive hermitian matrices. Here, the action of an effect on a state is defined by the Hilbert-Schmidt inner product. The unit effect is the identity matrix and normalized states have trace one.

3. Post-quantum cryptography

The motivation for wanting to consider theoretical frameworks beyond that of quantum theory is entirely legitimate. If for no other reason than the fact that Shor's algorithm revealed fundamental implications for classical notions of security, we can be justified in wanting to ensure nothing is lurking around the quantum corner (Shor 1994). While quantum theory has been validated time and again, it is conceivable that some future experiment may expose some limitation. This practical concern provides a compelling argument to investigate post–quantum theories and their effects on quantum theory. To this end, the formulation of general probabilistic theories have helped to uncover natural alternatives to quantum theory. For instance, in Boxworld we have a theory which admits all non–local, non–signalling correlations. We caution that theories of this type may be superseded by superluminal signalling theories.

Standard quantum key distribution schemes have been proven robust within realistic environments. Interestingly, this robustness has only been demonstrated with respect to possible attacks on the quantum information exchanged during the protocol. On the other hand, there is an assumption that the eavesdropper possesses all knowledge of classical information exchanged.

Furthermore, sources of classical randomness used in standard QKD protocols are implicitly assumed to be unbiased and completely inaccessible to the eavesdropper. Bouda *et al.* 2012 argued that perfect randomness is, in fact, unrealistic and that information eventually leaks via side channels, rendering it potentially vulnerable to the eavesdropper. As a result, Bouda *et al.* 2012 showed that the admission of weak randomness negatively influences the security of typical QKD protocols. It is precisely against this result, and the subsequent role of weakly random stochastic processes, that we question the security levels of more recent key distribution schemes. We shall now present a version of Barrett *et al.*'s construction, before going on to outline how this approach may allow an analysis of weak stochastic sources on the robustness of the construction, thereby taking into account all real-world practical threats.

Let us assume access to a d–dimensional irreducible state cone $\mathcal{S}_+$. Given a set of d linearly independent pure states $\{s_1, \ldots, s_d\}$, any measurement on this set will either disturb at least one of the states or provide zero information in which case, we have a non–disturbing measurement.

Protocol 1: A post-quantum key distribution scheme

Let us suppose that a communicating party wishes to discuss in a manner that is secure from arbitrary attacks by a post–quantum eavesdropper. The various stages of the corresponding protocol are as follows:

1. The first half of the communicating party, Alice, prepares a set of k *key* systems, each of which is randomly assigned to a state from the set $\{s_1, s_2\}$. Following this, Alice prepares a set of n *test* systems, each of which is randomly assigned to a state from the set $\{s_1, \ldots, s_d\}$. Alice then sends all $n + k$ prepared states in some random order to the second half of the communicating party, Bob;
2. On successful receipt of the communicated set of $n + k$ states, Alice announces those states that were originally assigned as key states and those that were assigned as test states;
3. On the set of test systems, Bob performs the measurement $\mathcal{M} = \{e_1, \ldots, e_d\}$ with $e_i, i = 1, \ldots d$ a linearly independent set. Alice and Bob abort the protocol on the occasion that any disturbance is revealed;
4. On the set of key systems, Bob performs the measurement $\mathcal{M} = \{e_1, e_2\}$ yielding

$$\begin{aligned} \langle e_1|s_2\rangle &= 0, \qquad \langle e_1|s_1\rangle > 0 \\ \langle e_2|s_1\rangle &= 0, \qquad \langle e_2|s_2\rangle > 0 \end{aligned}$$

5. As the protocol has proceeded to stage 4, the resulting outcomes can be used to obtain the secret key, whereupon s_1 can be taken as 0 and s_2 can be taken as 1.

4. Modelling weak stochastic processes

Within quantum key distribution, research has demonstrated the absolute necessity of perfectly random processes to theoretically guarantee the secrecy of quantum transmissions – a secrecy that, remarkably, is not vulnerable to technological progress. Within entanglement theory, meanwhile, findings have illustrated how the manipulation of perfect randomness implies computational and cryptographic tasks for which no classical analogues exit. Perfect randomness is ubiquitous and, thus, quantum technologies have been dominated by this strict and expensive assumption, despite that fact that devices may show a significant bias in their outputs. We shall now outline a technique by which we can use this fact as a basis to model the sources of randomness employed in the protocol above. By taking this line of argument, we hope to reveal an understanding of how random processes possibly impact the protocol.

Sources of randomness are described by probability distributions, and the ideal source of randomness for almost all protocols is the perfectly random source. However, perfect randomness is very difficult to obtain in practice, and so we argue that a more appropriate model of

randomness is that of weak randomness. Weak randomness has been extensively studied and is well understood in classical information processing, see, for example, Dodis *et al.* 2004, Maurer and Wolf 1997, and Renner and Wolf 2003. In light of this, we assume that a source exhibits randomness to some degree. Thus, we allow the outputs of such a source to be distributed according to any probability distribution displaying an adequate level of randomness. For what follows, we shall quantify the amount of randomness of a distribution by the *min–entropy* of its source. The min–entropy of the random variable $\mathbf{X}$ is defined by

$$H_\infty(\mathbf{X}) = \min_{x \in \mathbf{X}} \left(-\log_2 Pr\left(\mathbf{X} = x\right)\right). \tag{4}$$

Min–entropy is a widely accepted measure of weak randomness, and possesses a varied list of highly desirable properties (McInnes and Pinkas 1991). Importantly, min–entropy is sufficiently general which means that many real–world stochastic sources can be defined in terms of a min–entropy source. A noteworthy property of this source is that it readily models the most general of information leaks. In particular, a fall in min–entropy directly relates to the the amount of information learned by an eavesdropper, and in fact, a relatively small min–entropy decrease may well yield a sizeable amount of information. Another aspect of min–entropy relates to expected sequences. Here, an eavesdropper may be able exclude some sequences completely, which may aid with the design of future attacks.

Some important min–entropy quantities that may be used to assess the relative security merits of protocol above are as follows. A weak source of randomness is said to be an (n, b)–*source* if it outputs n–bit strings that are drawn according to a probability distribution with a min–entropy of at least b bits. Therefore, n–bit sequences have associated probabilities less than or equal to 2^{-b}. A perfect source occurs in the instance $b = n$. The *min–entropy loss* describes the bias of the source and is denoted $c = n - b$. We have an (n, b)–*flat distribution* if we have an (n, b)–source that is uniform on a subset of 2^b strings. The *min–entropy rate* is given by the quantity b/n, which achieves unity for perfectly random sources that deliver one bit of entropy per bit produced. Finally, particular interest lies with the *min–entropy loss rate*, which is denoted by quantity c/n. All of these quantities could prove to be very fruit tools when considering the real–world implementation key distributions protocols, including those known to be robust against general post-quantum eavesdroppers.

5. Future work and conclusion

In this paper, we have discussed a new topic of study called generalized probabilistic theories, which paves the way for a more robust discussion of physical systems should limitations to quantum theory be ever revealed. An interesting aspect of this discourse relates to cryptography and general security matters. Here, we outlined a novel approach for assessing the security parameters of cryptographic key distribution protocols that are known to be robust against general post–quantum attacks.

References

Barrett J, Hardy L and Kent A 2005 *Phys. Rev. Lett.* **95** 010503
Bouda J, Pivoluska M, Plesch M and Wilmott C 2012 *Phys. Rev. A* **86** 062308
Dodis Y, Jin Ong Shien, Prabhakaran M and Sahai A 2004 *Proc. 45th Ann. IEEE Symp. Found. Comp. Sci.* (IEEE Computer Society, Washington, USA) p 196.
Maurer U and Wolf S 1997 *Lect. Notes Comput. Sci. 1294, 307*
McInnes J L and Pinkas B 1991 *Proc. CRYPTO '90*
Popescu S and Rohrlich D 1994 *Foundations of Physics* **24** 3
Renner R and Wolf S 2003 *Lect. Notes Comput. Sci. 2729, 78*
Shor P 1994 *Proc. 35th Ann. Symp. on Foundations of Computer Science* (Santa Fe, NM)