A quantitative algebraic analysis of BB'84 with maximal entropy

Mehrnoosh Sadrzadeh[*]

Oxford University Computing Laboratory

Abstract

The paper provides a quantitative algebraic analysis of a BB'84-type quantum key distribution protocol. The analysis is done in an algebraic setting, where classical and quantum variables form a module for the quantale formed from the communication and quantum actions. The module-quantale pair is endowed with sup-maps that encode uncertainties of agents involved in the protocol, about the variables and about the actions. The right adjoint to the action of the quantale on the module provides a dynamic modality, read as "after". The right adjoints to the uncertainty maps provide epistemic modalities, read as "belief" of agents. Using these and the axioms of the algebra, we can express and verify whether the agents share a secret after running the protocol. The need for probabilities is felt, since in the presence of an intruder, agents cannot fully share their secret. We enter quantities into the analysis via degrees/probabilities of belief. These probabilities are derived from the number of choices that an agent has about actions and propositions involved in the protocol, these include actions of an intruder. For simplicity, we have assumed that the choices have a uniform chance of happening, hence as if assuming that the entropies of agents' choice sets are maximal. Using these probabilities, we show how the purpose of the actions in the protocol is to increase the agents' degrees of belief and to decrease the intruder's degree of belief. We show how a classical version of the protocol, in which the intruder can copy the passing qbit, is less efficient, since the intruder is able to obtain a higher degree of belief there. We also show how *security amplification*'s role is to decrease the intruder's degree of belief.

Introduction

In the world of logic, given any protocol, one aims to write down its properties in the form of a logical formula or algebraic term and prove its correctness using the axioms or rules of the logic or algebra. Quantum key distribution (QKD) protocols are no exception. A protocol is a sequence of events that change the values of the quantum and classical bits involved, hence the logic needs to be a dynamic one. If the protocol is correct, the agents involved in it will share a secret after running it, this means that they will acquire exclusive access to a piece information, e.g. the value of a bit. So a dynamic epistemic logic or

[*] mehrs@comlab.ox.ac.uk. Support from EPSRC grant EP/F042728/1 is gratefully acknowledged.

algebra seems to provide an appropriate setting. Examples of such logics are DEL of [1] and its more general algebraic version of [2]. In both articles simple examples of reasoning about security protocols have been presented. In fact, these examples constitute (alongside epistemic puzzles) the most appropriate motivation behind development and raison-d'etre of creation of such logics.

Indeed reasoning about quantum phenomena needs extra care because of the sophisticated nature of the rules thereof and only experts of the field have the eligibility to attempt to formalize it. But the subject is very attractive and its challenges are too tempting, so many non-experts have also taken their hinges, especially in the field of quantum information. Various less complex fragments of the theory have been isolated and different axiomatics and rule-based process calculi and logical systems have been developed for these simpler fragments, examples of such are the measurement calculus of [5] and a distributed version of it [4].

The dynamic epistemic logic approach has a nice axiomatics, based on adjoint modalities, to unfold correctness properties of any protocol. The distributed measurement calculus approach has the rules of a simple universal family of quantum measurements. In a contribution to a previous QPL in Iceland [3], the forces of these two systems were joined and a decision procedure to reason about QKD protocols was developed. The effectiveness of the procedure was demonstrated by modeling and reasoning about simple bi-partite secret sharing protocols in the style of Ekert'91 and BB'84, but also newer more complicated protocols on multi-agent secret sharing, based on graph states [6]. The need for probabilities were felt and their absence promptly criticized by the referees. Here, I do not claim to have overcome that problem but am trying to discuss some rough ideas on how one might go about to do so, by solely considering the dynamic epistemic part. This abstract is work in progress and perhaps should only be considered as a short contribution; it is based on a poster presented in [7].

A snapshot of the formalism

We model the correctness properties of a protocol as inequalities of an atomic sup-lattice M of propositions $m \in M$. The atoms of M are classical and quantum variables s_i^j and q_i, and the tensor product of quantum variables $q_l \otimes q_w$. The sup-lattice M is the right module of an atomic quantale Q, whose atoms are $N_l^{A,\gamma,i}$ for $\gamma \in \{X, Z\}$ denoting preparation of qbit l by agent A in basis X or Z for classical value $i \in \{0, 1\}$, or $P_l^{A,\gamma,i}$ denoting measurement (or projection) of qbit l by agent A in base X or Z and observing classical result i, or $E_{l,k}^A$ an entanglement of qbits l and k by agent A. The atoms also include communication actions such as public announcement of a proposition $m!?$, or a private announcement $m!?_\beta$ to a subgroup β of agents, or a more refined separate send $m!^{A\to B}$ and receive $m?^{B\leftarrow A}$ action. The pair (M, Q) is moreover required to satisfy the rules of distributed measurement calculus, as described in [3]. The action of Q on M is denoted by $- \cdot -\colon M \times Q \to M$, preserves all the joins of M, so has a right adjoint in its first argument $[q]-$, standing for the dynamic modality which is read as "after running protocol q, proposition m becomes true". These modalities yield weakest preconditions of program verification logics such as Hoare logic and PDL.

As established and elaborated on in previous work [2, 3], the pair (M, Q) of module-quantale, are endowed by sup-maps $f_A = (f_A^M, f_A^Q)$ where $f_A^M : M \to M$ and $f_A^Q : Q \to Q$, stand for uncertainties or possible choices of agents about the propositions or actions. For instance $f_A^M(m)$ is the uncertainty of agent A about proposition m, i.e. all the propositions that appear to agent A as true while in reality m holds. Similarly $f_A^Q(q)$ is all the actions that appear to agent A as happening when in reality q is happening. We ask the tuple (M, Q, f_A) to satisfy three f_A axioms of $f_A^M(m \cdot q) \leq f_A^M(m) \cdot f_A^Q(q)$, also that $f_A^Q(q) \leq f_A^Q(q) \bullet f_A^Q(q')$ and $1 \leq f_A^Q(1)$. Since each such f_A preserves all the joins, it has a Galois right adjoint, we focus on the one for f_A^M, denote it by $\Box_A m$ and read it as the belief modality, i.e. as ”agent A believes in proposition m”.

A uniform probability distribution is literally sitting in the setting. Since both M and Q are atomic, each element therein can be written as the join of atoms below it, i.e. $f_A(x) = \bigvee_{i=1}^{n} \alpha_i$ for $\alpha_i \in At(M)$. Now if k out of n of the atoms in $f_A(x)$ are less than or equal to a certain x', we say that with probability (at least) $\frac{k}{n}$ the uncertainty of agents about x satisfies x', that is (at least) k out of n of A's possible choices about x satisfy x'. We use this idea to introduce a new modality $\Box_{A,\frac{k}{n}} m'$, read as ”with probability (at least) $\frac{k}{n}$ agent A believes in m'”. We define this modality via the following rule

$$m \leq \Box_{A,\frac{k}{n}} m' \qquad \text{iff} \qquad f_A(m)_k \leq m'$$

where there is n atoms in $f_A(m)$ and k of them are $\leq m'$, hence their join is, that is $f_A(m)_k = \bigvee_{i=1}^{k \leq n} \alpha_i \leq m'$. This modality is used alongside the dynamic one: given the sequence of actions of a protocol π, and the initial situation that holds before it $Init$, we aim to prove

$$Init \quad \leq \quad [\pi]\Box_{A,\frac{k}{n}} m$$

That is, after running protocol π on the initial situation expressed in proposition $Init$, with probability (at least) $\frac{k}{n}$ an agent A believes that proposition m holds. By unfolding the dynamic adjunction and applying the above probability rule, this is iff k out of n of A's choices about the update of the initial property are $\leq m$, i.e. $f_A(Init \cdot \pi)_k \leq m$. To solve this inequality, one should first unfold $f_A(Init \cdot \pi)$, exactly as in the non-probabilistic setting, and obtain a join of n updated disjuncts which now constitute of atomic propositions and actions. One then goes on to check if k of them are $\leq m$, if so, the conclusion is that the original inequality holds. This easily yields a decision procedure, enhancing that of previous work.

The above treatment assumes a uniform distribution on atoms, as we are assuming that each atom in $f_A(x)$ has the same chance of happening. It is as if we are defining a measure $\mu(f_A(m))$ on M and set it to be n iff $f_A(m) = \bigvee_{i=1}^{n} \alpha_i$, which is the same as saying that each atom α_i of a choice cluster $f_A(m)$ has probability distribution $\frac{1}{\mu(f_A(m))}$. Toying with known concepts such as entropy, we recall that in some way entropy provides a measure for the distribution of choice and maximal entropy is when this distribution is uniform. So one can do a literal analogy and define that A's maximal entropy of his uncertainty about m to be equivalent to $-log(\mu(f_A(m)))$. One can elaborate on this a bit and define A's maximal entropy of m *shaded by* m' to be $\frac{k}{n} \times -log(\mu(f_A(m)))$ where k is $\mu(f_A(m) \wedge m')$ and n is $\mu(f_A(m))$. Now our above definition of probabilistic belief can be restated as $m \leq \Box_{A,\frac{k}{n}} m'$ iff A's maximal entropy of m shaded by m' is $(\frac{k}{n}) \times \frac{1}{-log(n)}$.

A lot more care needs to be taken for these probabilities or measures, but as we shall see below, these rough and simple-minded probabilities provide us with preliminary means to analyze QKD protocols in a nice numeric way, yet in a symbolic logical setting. They are also helpful in establishing a way to distinguish the effectiveness of quantum protocols versus that of their classical versions.

Example

Consider a simplified version of the BB'84 protocol where the measurements are restricted to X or Z. Alice prepares qbit q_1 and sends it to Bob, who upon receipt measures it. Then Alice publicly announces his preparation basis, if this is the same as Bob's measurement bases, then (in an ideal world, when there is no intruder) they share a secret, namely the classical result of the measurement. An ideal run of this protocol where the chosen basis of both agents is X would be as follow:

$$\pi = N_1^{A,X,1}; q_1!^{A\to B}; q_1?^{B\leftarrow A}; P_1^{A,X,1}; X!?^{A\to B}$$

Take s_l^i for $i \in \{0,1\}, l \in \{1,2\}$ to stand for the classical value i of measuring qbit l. If there was no intruder, we would have had the following right hand side for the correctness property of this protocol

$$[\pi]\left(\Box_{A,1} s_1^1 \wedge \Box_{B,1} s_1^1 \wedge \Box_{B,1}\Box_{A,1} s_1^1\right)$$

But the real world has intruders. Let's assume that we have only one of them called Eve, and that she is only intercepting the quantum channel and can measure A's sent qbit, then prepare another qbit according to the basis he chose for measurement and the result he saw, then send that to Bob, pretending it is from Alice. In this world, the above run of the protocol changes to the following one:

$$\pi = \underbrace{N_1^{A,X,1}; q_1!^{A\to B}; q_2?^{B\leftarrow A}; P_1^{A,X,1}}_{\sigma}; X!^{A\to B}$$

where Alice's sent qbit is q_1, but Bob's received one is q_2, which may or may not have been tampered with by E. The correctness properties of the protocol change accordingly, it is no more the case that the belief modalities have probability 1. In fact, our probabilities can be used to demonstrate how belief degrees increment as a result of the protocol actions. For instance, take σ to be the sequence of actions just before A publicly announces her basis. Then we have the following property:

$$[\sigma]\left(\Box_{A,7/12}\, s_1^1 \wedge \Box_{B,7/12}\, s_1^1 \wedge \Box_{A,7/12}\Box_{B,7/12} s_1^1\right)$$

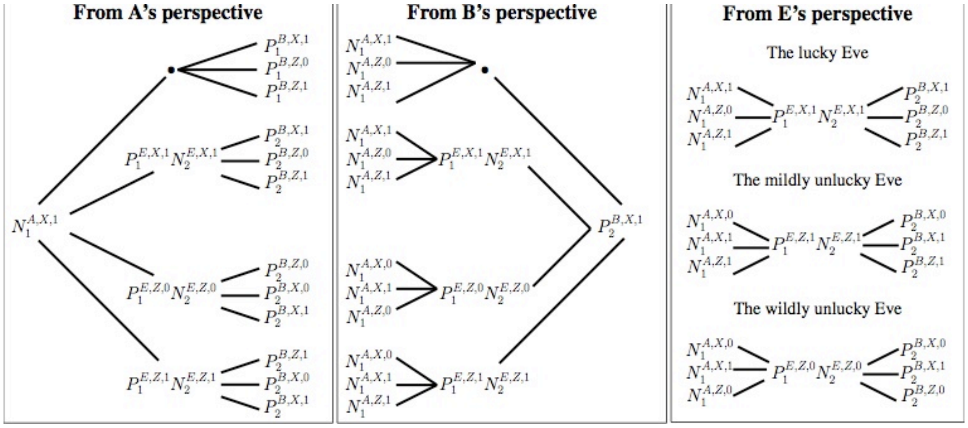
We also obtain the following properties regarding Eve's belief

$$[\sigma]\left(\Box_{E,5/9}\, s_1^1 \wedge \Box_{A,9/12}\Box_{E,5/9}\, s_1^1 \wedge \Box_{B,9/12}\Box_{E,5/9}\, s_1^1\right)$$

The purpose of Alice's classical communication action at the end of the protocol is to increase the belief probability of Bob, which unfortunately will also increase that of Eve with exactly the same amount. This is demonstrated by verifying the following properties

$$[\pi]\left(\Box_{B,4/6} s_1^1 \wedge \Box_{E,2/3} s_1^1\right)$$

However if the classical communication only happens as a private announcement between A and B, Eve's belief degree will stay $5/9$ where as Bob's will change to $4/6$. These properties are verified, by counting the possibilities of the agents and checking that in which one of them s_1^i has $i = 1$. Here the non-identity uncertainties are those of each agent about the actions of the others. For example when Alice does an $N_1^{A,X,1}$ preparation and Bob does a $P_2^{B,X,1}$ measurement, Bob thinks that Alice might have done either of $N_1^{X,1}, N_1^{Z,0}, N_1^{Z,1}$, i.e. we have $f_B(N_1^{A,X,1}) = N_1^{X,1} \vee N_1^{Z,0} \vee N_1^{Z,1}$. The uncertainties of a sequential composition of actions, break down to uncertainties of atoms by join preservation of sequential composition in Q and the axioms of f_A's. At this stage of the protocol, the choices of Eve are exactly the same. We have enumerated these choices of the actions in the run σ in the trees below:

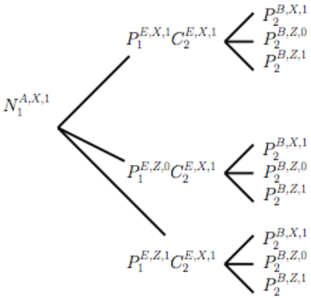


We see that for example, the total number of Bob's choices are 12 and in 7 of them s_1^i has $i = 1$, hence after σ Bob will believe that with probability $7/12$ the value of Alice's prepared bit was 1. Similarly, Eve has 9 choices in total and in 5 of them s_1^i has $i = 1$. After the classical public announcement of X by Alice, the axiomatics makes sure that the branches of the trees that have a Z measurement will be eliminated, hence the total possibilities of, e.g. Bob will now become 6, out of which 4 have s_1^1.

Exactly because of the possible presence of intruders, quantum protocols do not run in just one round. As we have seen above, were this the case, Alice and Bob could not be sure that they share a secret. So these protocols are ran in many rounds, after which Alice and Bob try to deduce which runs were tampered with by the intruder, throw those runs away, and take a function, like xor of the classical bits of the resulting runs and make that their secret. This process is referred to as *security Amplification*.

We think of security amplification as being useful, since it increases the probability of Alice and Bob's beliefs and decreases that of Eve. Verifying this involves the tedious task of forming the above tree for each run of the protocol and put the trees side by side. Assume Alice and Bob run the protocol twice and form the xor of the results, then one can verify that if Eve is lucky, i.e. restrict her choices to those of the top tree demonstrated above, then his degree of belief decrease from $5/9$ to $4/9$. Working a bit harder and running the protocol four times, then making Alice and Bob take the xor's of the results of the first two rounds and the second two rounds separately, then taking the conjunction of these, one can show that Eve's belief probability decreases to $6/27$.

Finally, let us imagine a classical version of the protocol and show that it is less effective, by for example showing that it increases Eve's degree of belief. One way to go classical is to suppose that Eve can actually copy the qbit that he is intercepting, i.e. action $C_2^{E,X,1}$. In this case his tree of possibilities will be as follows:



Here after running σ, Eve's degree of belief increases from $5/9$ to $6/9$, hence the classical version is less efficient than the quantum one.

Addendum and Acknowledgement

Just a final note, that here we have introduced a very naive notion of probabilistic belief in an algebraic setting, which probably suffers from very many shortcomings. But developing a full blown logic with these modalities has not been the aim of this abstract. We have tried to keep things simple and to demonstrate that even with these simplistic assumptions, a great deal can be said about quantum protocols just by deriving the degrees of beliefs of the agents involved in them. In preliminary discussions with P. Panangaden, he pointed out that these can be organized and generalized, by for example assigning a measure to each atom externally, as opposed to computing it internally by counting. Such a generalization, also investigating the derivation power of the probabilistic modalities is of course a necessity and hopefully will constitute the subject of joint future work. Support by EPSRC (grant EP/F042728/1) is gratefully acknowledged.

References

[1] A. Baltag and L.S. Moss. 'Logics for epistemic programs'. *Synthese* **139**, 2004.

[2] A. Baltag, B. Coecke, and M. Sadrzadeh, 'Epistemic actions as resources', *Journal of Logic and Computation* **17 (3)**, May 2007, `arXiv:math/0608166`.

[3] E. D'Hondt and M. Sadrzadeh, 'Classical Knowledge for Quantum Security', to appear in *ENTCS* Proceedings of Joint QPL-DCM workshop, ICALP, July 2008.

[4] V. Danos, E. D'Hondt, E. Kashefi, and P. Panangaden, 'Distributed measurement-based quantum computation', in *ENTCS Proceedings of the 3rd QPL*, 2005.

[5] V. Danos, E. Kashefi and P.Panangaden, 'The measurement calculus', *Journal of the ACM*, 54(2), 2007.

[6] D. Markham, A. Roy and B. Sanders, 'Graph States for Quantum Secret Sharing', *Physical Review* **78, 042309**, 2008.

[7] 'A Maximal Entropy Analysis of Degrees of Information in Quantum Protocols', Poster presented in *QICS European Project Workshop on Foundational Structures for Quantum Information and Computation*, Austria, 2008.