An Epistemic Measurement System for Quantum Security

An Epistemic Measurement System for Quantum Security

Elham Kashefi
Oxford University
kashefi@comlab.ox.ac.uk

Mehrnoosh Sadrzadeh
University of Southampton
ms6@ecs.soton.ac.uk

We develop a formal system to reason about knowledge properties of quantum security protocols. The formalism is obtained via a marriage of measurement calculus [3], an algebraic framework for measurement-based quantum computing [7], with the algebra of epistemic actions and their *appearance maps* [1, 8].

Measurement calculus has also proven to be a proper language to describe and to analyse distributed quantum protocols [4]. Protocols (here referred to as measurement pattern) are described by a combination of commands: 1-qubit preparations N_i (prepares qubit i in state $|+\rangle_i$), 2-qubit entanglement operators $E_{ij} := \wedge Z_{ij}$ (controlled-Z operator), 1-qubit measurements M_i^α, and 1-qubit Pauli corrections X_i and Z_i, where i, j represent the qubits on which each of these operations apply, and $\alpha \in [0, 2\pi)$. Measurement M_i^α is defined by orthogonal projections $P_i^{|+_\alpha\rangle}$ (with outcome $s_i = 0$) and $P_i^{|-_\alpha\rangle}$ (with outcome $s_i = 1$). [1] Dependent corrections, used to control non-determinism, will be written $X_i^{s_j}$ and $Z_i^{s_j}$, with $X_i^0 = Z_i^0 = I$, $X_i^1 = X_i$, and $Z_i^1 = Z_i$. Any pattern can be put in a standard form, where all the preparation and entanglement can be done first, followed by local measurements and corrections and classical communications. The initial entanglement state is the distributed global memory shared among the agents at the beginning of the protocol and the classical outcome of measurements represents the classical communication of agents.

The starting point is our main result that proves the *well-defined* measurement patterns with *flow* [2] form a quantale Q. Recall that a quantale is a sup-monoid $(Q, \leq, \bigvee, \bullet, \epsilon)$ where in our case the monoid multiplication is the sequential composition (or juxtaposition) of measurement pattern commands. In the fragment of measurement patterns with flow, probabilities of each branch of measurement are equal, as a result a measurement can be written as the non-deterministic choice of its projections, that is $M_i^\alpha = P_i^{|+\alpha\rangle} \vee P_i^{|-\alpha\rangle}$. The induced order is the non-deterministic order of information between each projection of the measurement, that is $P_i^{|+\alpha\rangle} \leq M_i^\alpha$ and $P_i^{|-\alpha\rangle} \leq M_i^\alpha$. We add agents $A \in \mathcal{A}$ to our quantale by endowing it with a family of lax quantale endomorphisms $f_A^Q \colon Q \to Q$, one for each agent $A \in \mathcal{A}$. We interpret $f_A^Q(q)$ as *appearance* of agent A about action q, that is all the actions that agent A considers as happening when action q is happening in reality. Since f_A^Q preserves all joins, it has a Galois right adjoints that preserves all meets. The adjunction is denoted by $f_A^Q \dashv \Box_A^Q$ and we read $\Box_A^Q\, q$ as 'agent A knows that action q is happening'. These maps and their relation to the traditional notions of knowledge and belief in epistemic logic have been studied in [1, 8].

Each action has an owner that generates the action, we encode the owner as the map $gen \colon Q \to \mathcal{A}$ and whenever $gen(q) = Q$, we use the shorthand q^A. For example, the generator of an entanglement action is the source that creates the entangled state. In this case, we distinguish the agents that share the state from the source via the shorthand $E_{i,j}^{C,A,B}$ where $inv(E_{i,j}^{C,A,B}) = (A, B), gen(E_{i,j}^{C,A,B}) = C$ and $inv \colon Q \to \mathcal{A} \times \mathcal{A}$ is defined partially on the entanglement actions. We use these maps to assign appearances to action for each agent. For instance, all actions appear as identity to their generators, that is $f_A(M_i^{\alpha,A}) = M_i^{\alpha,A}$.

We assume that the right module M of our quantale Q is the lattice of results of measurements. The action of the quantale on the module $- \cdot - \colon M \times Q \to M$ stands for the change of the state of a system as a

[1] Here $|\pm_\alpha\rangle$ stand for $\frac{1}{\sqrt{2}}(|0\rangle \pm e^{i\alpha}|1\rangle)$.

result of a measurement pattern. The Galois right adjoint to this operation on its first argument $- \cdot q \dashv [q]-$ is the dynamic modality or the *weakest precondition* of Hoare logic. Similar to the Q, We endow M with a family of join preserving maps $f_A^M \colon M \to M$ and interpret them as appearance of agents about results of measurements. The pair (f_A^M, f_A^Q) is moreover asked to be a *lax system endomorphism*. We call the whole formalism $(M, Q, \{(f_A^M, f_A^Q)\}_{A \in \mathcal{A}})$ an *epistemic measurment system*, built on the notion of epistemic systems defined in [1, 8].

Ekert'91. As an example, we encode and reason about the Ekert'91 protocol [6] and an attack on it. The measurement pattern of the protocol is as follows

$$Ek := (s_4!^B)(s_3!^A)(M_2^{B,s_4(\frac{\pi}{2})} M_4^{B,\frac{\pi}{2}} N_4 M_1^{A,s_3(\frac{\pi}{2})} M_3^{A,\frac{\pi}{2}} N_3^A) E_{1,2}^{C,A,B}$$

where $x!$ is the public announcement of x in a classical channel. We show that for s_1 and s_2, the results of measurements on qbits 1 and 2 respectively, if the source of entanglement is trustable and the protocol is successful, *i.e.* $s_3 = s_4$, then agents A and B *share* a *secret*. Sharing is expressed via the following inequalities (leading to common knowledge between A, B), e.g. the fist one says that after a successful run of the protocol, A knows the result of B's measurement:

$$\top \leq [Ek]\Box_A\, s_2, \qquad \top \leq [Ek]\Box_B\, s_1, \qquad \top \leq [Ek]\Box_B \Box_A s_2, \qquad \top \leq [Ek]\Box_A \Box_B\, s_1$$

Secrecy is expressed via the following inequalities for all other agents $X \neq A, B$, e.g. after a successful run of the protocol, X does not know the result of A and B's measurements and A and B are aware of this:

$$\top \leq [Ek]\neg\Box_X\, s_1, \qquad \top \leq [Ek]\neg\Box_X\, s_2, \qquad \top \leq [Ek]\Box_A \neg\Box_X\, s_1, \qquad \top \leq [Ek]\Box_B \neg\Box_X\, s_2$$

However, if the source of entanglement is not trustable we can show the opposite of above properties, e.g.

$$\top \leq [Ek]\neg\Box_A\, s_2, \qquad \top \leq [Ek]\neg\Box_B\, s_1$$

Related and Future Work. Another attempt to use measurement calculus to reason about properties of distributed quantum protocols has been originated in [4] and further elaborated on in [5]. Our approach differs from these in that we work in an algebraic, rather than relational, setting and moreover our knowledge is not based on the equivalence of states. As a consequence we can also reason about misinformation actions such as the faulty Bell pair in the attack to the Ekert protocol. As future work, we aim at analyzing further examples to demonstrate the powers and limitations of our approach. We would like to investigate how our right module is generated, for example as the lattice of closed subspaces of the Hilbert space consisting of the tensor product of the systems involved in a protocol. The generalization of appearance maps to the minimal and canonical join to reason about the general class of quantum key distribution protocols is our other aim. Finally, we would like to implement our algebra as a mechanized software tool.

References

[1] A. Baltag, B. Coecke, M. Sadrzadeh, 'Epistemic actions as resources', *Logic and Computation*, to appear.

[2] V. Danos, E. Kashefi, , 'Determinism in the one-way model', *Phys. Rev. A.* **74**, 2006.

[3] V. Danos, E. Kashefi, P. Panangaden, 'The Measurement Calculus', *Journal of ACM*, to appear.

[4] V. Danos, E. D'Hondt, E. Kashefi, P. Panangaden, 'Distributed measurement-based quantum computation', Proceedings of QPL 2005.

[5] E. D'Hont, P. Panangaden, 'Quantum Knowledge', Proceedings of FSTTCS05, *LNCS* **3821**, 2005.

[6] A.K. Ekert, 'Quantum Cryptography Based on Bell's Theorem', *Phys. Rev. Lett.* **67**, 1991.

[7] R. Raussendorf, H.J. Briegel, 'The one-way quantum computer', *Phys. Rev. Lett.* **86**, 2001.

[8] M. Sadrzadeh, 'Actions and Resources in Epistemic Logic', Ph.D. Thesis, University of Quebec at Montreal, 2006.