An Epistemic Measurement System for Quantum Security

Citation for published version:

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Peer reviewed version

Published In:
International Iran Conference on Quantum Information 2007

General rights
Copyright for the publications made accessible via the Edinburgh Research Explorer is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The University of Edinburgh has made every reasonable effort to ensure that Edinburgh Research Explorer content complies with UK legislation. If you believe that the public display of this file breaches copyright please contact openaccess@ed.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.
An Epistemic Measurement System for Quantum Security

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

Mehrooosh 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 \( |+\rangle \)), 2-qubit entanglement operators \( E_{ij} := \Lambda Z_{ij} \) (controlled-Z operator), 1-qubit measurements \( M_i^\alpha \), 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 \( M_i^\alpha \) is defined by orthogonal projections \( P_i^{\alpha,+} \) (with outcome \( s_i = 0 \)) and \( P_i^{\alpha,-} \) (with outcome \( s_i = 1 \)). Dependent corrections, used to control non-determinism, will be written \( X_i^\alpha \) and \( Z_i^\alpha \), 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 is happening in reality. Since \( s_i \) 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 \( gen(q) = Q \), 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 \( inv : Q \rightarrow A \times A \) 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 \( \cdot : M \times Q \rightarrow M \) stands for the change of the state of a system as a

---

\[ 1 \] Here \( |\pm\rangle \) 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 $\cdot q \vdash [q]$ 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 $f^M_A : M \to M$ and interpret them as appearance of agents about results of measurements. The pair $(f^M_A, f^Q_A)$ is moreover asked to be a lax system endomorphism. We call the whole formalism $(M, Q, \{ (f^M_A, f^Q_A) \}_{A \in A})$ an epistemic measurement 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

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

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 qubits 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:

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

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:

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

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

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

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