Available online at www.sciencedirect.com
ScienceDirect
Electronic Notes in Theoretical Computer Science
ELSEVIER
Electronic Notes in Theoretical Computer Science 270 (1) (2011) 155–163
www.elsevier.com/locate/entcs

Classical Knowledge for Quantum Security

Ellie D'Hondt[2]

Vrije Universiteit Brussel & FWO, Belgium

Mehrnoosh Sadrzadeh [1]

Laboratoire Preuves Programmes et Systèmes, Université Paris 7, France

Abstract

We propose a decision procedure for analysing security of quantum cryptographic protocols, combining an algebraic logic rewrite system with an operational semantics for quantum distributed computations. We apply our approach to reasoning about security properties of a recently developed quantum secret sharing protocol.

Keywords: Quantum cryptography, distributed measurement calculus, algebraic information update.

1 Introduction

Quantum communication is an inseparable part of quantum computing: it offers solutions to the risks caused by exponential speed-up in the power of an adversary as a result of quantum algorithms. While some advances have been made in the area of formal verification of quantum communication protocols [11], no applicable formal framework has yet been suggested for their automatic cryptanalysis. This is contrary to the fact that, similar to the situation in classical security, attacks have been discovered on proven-to-be-safe quantum protocols. In this paper we present a decision procedure that verifies whether a protocol satisfies a security property by deriving knowledge properties of its agents on the dynamic and epistemic traces of the protocol. The *dynamic traces* are generated from the specification of a protocol using the operational rules of distributed measurement calculus [5] (DCM). These are then expanded to the *epistemic traces* using appearances of agents about the actions of the protocol. The appearances are derived from the safety assumptions of

[1] Email: mehrs@comlab.ox.ac.uk
[2] Email: Ellie.DHondt@vub.ac.be

doi:10.1016/j.entcs.2011.01.014

the communication channels according to a set of rules. Our notions of knowledge and time are classical and have been used in formal analysis of classical protocols, for example in Halpern style models of [14,7] and in dynamic epistemic algebra of [2,17].

Both the DCM model and the algebra have been previously used to analyze the security of quantum key distribution (QKD) and its attacks [8,7,16]. The setting of this paper has advantages over both these attempts. First, we rely on the already existing rules of the semantics of DMC, as opposed to adding axioms for quantum mechanics to the algebra. Second, we use the algebraic axiomatics of adjunction to derive knowledge properties of the protocol, as opposed to model-checking them by traversing the tree of the protocol. Third, we set the actions of the adversary in a compositional way using the appearance maps of the algebra, as opposed to adhocly adding them to the specification of the protocol. We prove that our decision procedure is sound and terminating with regard to the pair of a DMC model and the algebraic axiomatics of Epistemic Systems. We apply our decision procedure to a new quantum secret sharing (QSS) protocol, which is based on graph states and has been proposed recently in [12]. For this protocol, we develop epistemic properties and prove them for three kinds of assumptions on the quantum channels: safe, unsafe with non-suspicious agents, and unsafe with suspicious agents. However, we can only work on a one-round basis and indeed, for a full analysis of protocols one needs to run the protocol in many runs and then use probabilities, for instance on the knowledge modalities. This would be a natural and exciting extension of the currently proposed framework.

In a nut shell, our framework is obtained by merging the model checking approach of [8,7] and the algebraic axiomatics of [16]. The former is based on a distributed extension [5] for an assembly language [6] that universally models computations of the one way model. Its knowledge operator is defined over Kripke structures in the style of Fagin et al [10] by using equivalence relations on the states. Reasoning about properties of a protocol is done on the state space of this structure using a logic with temporal and epistemic operators. The latter is based on the Stone-like duals of these relational systems and moreover, following [4], a quantale structure is assumed on the actions. This setting consists of a pair of a quantale of classical and quantum actions and its right module of bits and qubits involved in a protocol. The pair is endowed with a family of join-preserving maps, one for each agent involved in the protocol. The right adjoints to these endomorphisms give rise to a very useful notion of knowledge, both on propositions of module and actions of quantale.

2 Decision Procedure

First, given the specification of a quantum protocol as a program in the language of the distributed measurement calculus (DMC), we generate its *dynamic traces* by executing the rules of the operational semantics. Second, we write the epistemic property we wish to prove about security of the protocol in the language of Epistemic

Systems. Finally, we apply our algebraic rewrite system to decide whether the protocol satisfies the property or not, The last step unfolds the appearances to agents of dynamic traces and adds new traces to the existing dynamic, to which we refer as *epistemic traces*.

Specify and trace in DMC. A *network of agents* $\mathcal{N}$ is defined by a set of agents acting in parallel (denoted by $|$) acting on a given entanglement resource $|\psi\rangle$,

$$\mathcal{N} = |\psi\rangle \parallel \mathbf{A}(Q).\mathcal{E} \mid \mathbf{B}(Q').\mathcal{E}' \dots \quad .$$

An *agent* $\mathbf{A}(Q).\mathcal{E}$ is specified by a name $\mathbf{A}$, a set Q of qubits it owns, and an event sequence $\mathcal{E}$ consisting of computations in the measurement calculus, classical message reception $\mathsf{c}?x$ and sending $\mathsf{c}!y$, and qubit reception $\mathsf{qc}?q$ and sending $\mathsf{qc}!q'$. Note that, contrary to the original definitions in [5] we now write specifications from left to right; also agents may have extra classical parameters a, written as $A(a, Q)$. As an example, here is one round of Ekert's implementation of QKD:

$$QKD = E_{12} \| \mathbf{A}(a,1).[H_1^a; M_1; \mathsf{c}!a; \mathsf{c}?b] \mid \mathbf{B}(b,2).[H_2^b; M_2; \mathsf{c}?a; \mathsf{c}!b] \ .$$

The set of traces of a program are generated by following the rules of the small-step semantics as specified in [5], but moreover, we work with projections, annotate actions with agents that performed them, and name the preparation actions of the initial entanglement resource $|\psi\rangle$. For example, $P_i^{A,\alpha}$ stands for the spin α projection of qubit i done by agent A. The preparation actions are made explicit by juxtaposing them to the left most of the traces; for QKD the entanglement resource E_{12} is created by applying $N_1; N_2; E_{12}$ to a 2-qubit system $q_1 \otimes q_2$, where N is preparation in the $|+\rangle$ state, and then distributing these qubits over agents A and B. Two of the four possible traces for a successful run of QKD are

$$\pi = N_1; N_2; E_{1,2}^{A,B}; P_1^{A,X}; P_2^{B,X}; \mathsf{c}!a; \mathsf{c}?a; \mathsf{c}!b; \mathsf{c}?b, \qquad \pi' = N_1; N_2; E_{1,2}^{A,B}; P_1^{A,Z}; P_2^{B,Z}; \mathsf{c}!a; \mathsf{c}?a; \mathsf{c}!b; \mathsf{c}?b \ ,$$

Reduce in Epistemic Systems. The input to the rewrite system is an expression of the form $l \vdash r$ where l is the initial state and r is an epistemic property that contains the disjunction of dynamic traces produced above. The expression $q_i \vdash [\pi]\Box_A\Box_A s_i^j$, reads as 'after running the trace π of the protocol on qbit q_i, agent A knows that B knows that the value of bit i is j'. The l and r expressions are generated as follows:

- The initial state l is made of propositions m that are formed by closing atomic classical and quantum variables s_i^j and q_i under $\neg, \wedge, \vee$ and logical constants $\bot, \top$, The variables are generated via $\kappa ::= s_i^j \mid q_l \mid q_l \otimes q_w$.
- The epistemic property r is generated via $r ::= m \mid [\pi]m \mid \Box_A(m)$, where $\Box_A(m)$ is the epistemic modality and for π a dynamic trace $[\pi]m$ is the dynamic modality.

One such expression for Ekert's QKD is

$$q_1 \otimes q_2 \vdash \left[N_1; N_2; E_{1,2}^{A,B}; P_1^{A,X}; P_2^{B,X}; \mathsf{c}!a; \mathsf{c}?a; \mathsf{c}!b; \mathsf{c}?b\right] \Box_A\Box_B(s_1^0 \wedge s_2^0)$$

Proving this property together with a permutation of it for the knowledge of B will imply that A and B *share* a piece of data. That the data is *secret* is proved by showing that an adversary E does not know it, that is the following expression

$$q_1 \otimes q_2 \vdash \left[N_1; N_2; E_{1,2}^{A,B}; P_1^{A,X}; P_2^{B,X}; \mathsf{c}!a; \mathsf{c}?a; \mathsf{c}!b; \mathsf{c}?b\right] \neg\Box_E(s_1^0 \wedge s_2^0)$$

We proceed by analyzing uncertainty of agents about the states and actions of protocols. These are referred to as *appearance* maps and are denoted by f_A for an agent A. They encode all possible actions or propositions that appear possible to an agent, given the action that is happening or the proposition that is true in reality and are set according to the general rules below.

(i) The agents have no uncertainty about the steps of the protocol they are involved in.

(ii) Qubits are encoded as black boxes and thus appear as the identity to all agents. Classical bits appear as either 0 or 1 to agents.

(iii) The owner of an action has no uncertainty about his actions, but is uncertain about other agents' actions. His appearances are generated by instantiating variables of these actions.

(iv) There is only one adversary present in each protocol. This adversary can intercept the unsafe channels, either quantum or classical, by stopping the messages, changing the content of the messages, creating new messages and sending them. On a quantum channel, the change of the content of the message is done by measuring the sent qbit and the creation of new messages by preparing fresh qbits. On the classical channel, the change is simply affected by reading and writing the values of the bits.

(v) On the safe channels, the adversary can either be passive or not present at all. In the latter case, he cannot even see if messages are passing through and what is their content. In the former case, on a classical channel, he can see the value of the bits passing by as well as the sender and receiver of each message, but cannot change anything. On a quantum channel, he can only see that a qbit is passing, but cannot see the state of it.

(vi) Communication actions on a safe channel are either public or private announcements to a subgroup of agents. The former appears as the identity to all agents, whereas the latter is identity only to the insiders in the group, and either as nothing or all possible choices to the outsider agents. On an unsafe channel these are broken to separate send and receive actions.

(vii) Honest agents may suspect the interception actions of the adversary. In case they do, these appear to them as either have happened or not. In case they do not suspect, they appear to them as the neutral action in which nothing happens.

For example the appearance of the projection action $P_1^{A,X}$ in our above trace are

$$f_A(P_1^{A,X}) = P_1^{A,X}, \qquad f_B(P_1^{A,X}) = P_1^{A,X} \vee P_1^{A,-X} \vee P_1^{A,Z} \vee P_1^{A,-Z} \quad .$$

Due to space limits we refrain from presenting the rewrite rules; they are similar to the system presented in [15]. By applying them, one first eliminates the logical connectives $\wedge, \vee, \Box_A, [\,]$ and then the classical and quantum communication actions. The output is a set of *atomic expressions*:

Definition 2.1 An expression $l \vdash r$ is atomic iff l is a quantum state followed by a sequence of atomic quantum actions and r is an atomic classical or quantum state.

For instance, for a safe quantum channel, the atomic form of the our sharing property is $(q_1 \otimes q_2)(N_1; N_2; E_{1,2}^{A,B}; P_1^{A,X}; P_2^{B,X}) \vdash s_1^0 \wedge s_2^0$. These atomic expressions contain new epistemic uncertainties and need to be verified against our operational semantics. Only then can we check if a protocol has a desired epistemic property.

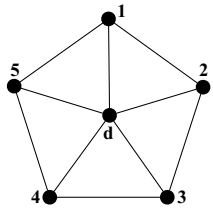
Definition 2.2 An atomic expression $l \vdash r$ is *well-defined* iff l is derivable within the operational semantics of DMC. It is true iff r holds in all configurations resulting from l. An epistemic property holds for a protocol whenever all its well-defined atomic expressions are true.

Proposition 2.3 *For a protocol specification $\mathcal{N}$ and a given expression $l \vdash r$ which is built from the dynamic traces of $\mathcal{N}$, the process of deciding if the epistemic property in r holds for $\mathcal{N}$ is terminating and sound with regard to the pair of an Epistemic System and a DMC model.*

Proof. These follow from image finiteness of appearances of actions and propositions, together with soundness and termination of the rewrite system of Epistemic Systems and the DMC model [5,15].

3 Case study: quantum secret sharing

We apply our procedure to the quantum secret sharing (QSS) protocol recently established in [12]. In secret sharing a dealer holds a secret bit which he wants to send to n players, such that at least k players are needed to reconstruct the secret. The problem is well-known in classical settings and solvable for all (n, k). In the quantum case, only the (n, n) case has been solved for the GHZ-type entanglement [18]. The work in [12] uses instead graph states and thus is more suitable for modelling in our measurement-based setting. Moreover, it generalizes the quantum key distribution protocols and simplifies their proofs. We analyze and prove some of the epistemic properties of the QKS component of the $(3, 5)$ case where a particular graph state is used to establish a secret key between three players and the dealer in one go (as opposed to via several 2-party QKD protocols). This key will then be used to distribute a secret using the other components of the protocol.



The resource required for the protocol is the graph state shown above, henceforward called $G(3, 5)$. It is prepared following the usual procedure for graph states, that is

$$G(3,5) = (N_1; \ldots; N_5; N_6; \prod_{e_{ij}} E_{ij}) \otimes_{i=1}^{6} q_i; ,$$

with e_{ij} the set of edges. The protocol proceeds as follows:

Step 1. The dealer prepares $G(3, 5)$, sends each agent a qubit q_i together with an agent identity i.

Step 2. The dealer measures in the Y or Z basis randomly and broadcasts his measurement basis.

Step 3. Each participating player measures in the X, Y or Z basis randomly, then broadcasts his identity and measurement basis.

Step 4. Depending on these messages, each agent determines if the run was successful. If the participating agents are neighbours, $ijk = i(i+1)(i+2)$, this is the case for measurement combinations

$$M_6^Z M_i^Z M_j^X M_k^Z \quad \text{and} \quad M_6^Y M_i^X M_j^Y M_k^X \ .$$

If they are in a so-called T-shape, $ijk = i(i+1)(i+3)$, the right measurement combinations are

$$M_6^Z M_i^X M_j^Y M_k^Y \quad \text{and} \quad M_6^Y M_i^Y M_j^Z M_k^Z \ .$$

Step 5. For a successful run, measurement outcomes are correlated as follows: $s_6 = s_i \oplus s_j \oplus s_k$. Players use their secure classical channels to exchange measurement outcomes and determine $s = s_6$, hence establishing a shared key with the dealer.

We refrain from giving the full specification of the QSS network and move straight on to its traces where we introduce the notation $a!^{\sigma}$ to stands for the broadcasting of the value a throughout the network by agent σ. The communica-

tion between the dealer and players can be listened to, while communication among players is secure and occurs through a handshake between operations $\mathsf{c}?$ and $\mathsf{c}!$ ($\mathsf{c}!?$ in short). We differentiate between both types of communication in our security analysis below. A typical trace for a successful run of QSS is as follows

$$\begin{array}{ll}
\pi = & N_1;\ldots;N_6;\prod_{e_{ij}} E_{ij} \quad \text{(preparation)}\\
& (\mathsf{qc}!?^D q_1)\ldots(\mathsf{qc}!?^D q_5) \quad \text{(distribution of qubits)}\\
& P_6^{D,\pm a} P_i^{A_i,\pm b} P_j^{A_j,\pm c} P_k^{A_k,\pm f} \quad \text{(measurement projections)}\\
& a!^D; b!^{A_i}; c!^{A_j}; f!^{A_k} \quad \text{(public broadcast of measurement bases)}\\
& (\mathsf{c}!?^{A_i}_{A_j,A_k} s_i)(\mathsf{c}!?^{A_j}_{A_i,A_k} s_j)(\mathsf{c}!?^{A_k}_{A_i,A_j} s_k) \quad \text{(private exchange of player measurement outcomes).}
\end{array}$$

Here $a \in \{X,Y\}, b,c,f \in \{X,Y,Z\}$ are measurement basis, $\mathsf{qc}!?^D_{A_i}$ is the quantum message passing from D to $A_i \in \{A_1,\cdots,A_5\}$ denoting the 5 players, and $\mathsf{c}!?^{A_i}_{\beta}$ is the private announcement from player A_i to the group $\beta \subseteq \{A_1,\cdots,A_5\}$. We omit the calculation of the secret key $s = s_i \oplus s_j \oplus s_k$. Successful traces depend only on the chosen values for a,b,c and e; one example for adjoining agents A_1, A_2 and A_3, owning qubits 1,2 and 3 respectively, is

$$\pi = \ldots P_6^{D,+Z} P_1^{A_1,-Z} P_2^{A_2,-X} P_3^{A_3,+Z} Z!^D; Z!^{A_1}; X!^{A_2}; Z!^{A_3}; (\mathsf{c}!?^{A_1}_{A_2,A_3}\ 1)(\mathsf{c}!?^{A_2}_{A_1,A_3}\ 1)(\mathsf{c}!?^{A_3}_{A_1.A_2}\ 0)$$

Epistemic Properties

We consider three cases: agents' heaven, adversary's heaven, and adversary's hell. In the first case the quantum channel is safe, in the second case it is not and the honest agents do not suspect it, in the third case it is not and the honest agents do suspect it. The other channels are assumed to be safe in both cases.

(i) **Agents' heaven**

The appearance of the projections are set according to rule (*iii*) of appearances. Since the channels are safe, the communication actions on the quantum channel are also treated as public broadcasts, i.e. for σ an agent we have $f_\sigma(\mathsf{qc}!?^D q_i) = \mathsf{qc}!?^D q_i$. The communication actions on the classical channels are private announcements, i.e. for a subset of players β we have

$$f_\sigma(\mathsf{c}!?^{A_i}_{\beta} s_i^j) = \begin{cases} \mathsf{c}!?^{\sigma}_{\beta} s_i^j & \sigma \in \beta \\ \mathsf{c}!?^{\sigma}_{\beta} s_i^j \vee \mathsf{c}!?^{A_i}_{\beta} \overline{s}_i^j & \sigma \notin \beta \end{cases}$$

Some of the epistemic properties of interest for our trace π, allied players $A_i \in \{A_1,A_2,A_3\}$, joined with dealer $\sigma \in \{D,A_1,A_2,A_3\}$ are as follows

- The dealer knows his bit and binary sum of allied players bits, $\Box_D\,(s_6^0 \wedge (s_1^{b_1} \oplus s_2^{b_2} \oplus s_3^{b_3}))$.
- Allied players moreover know the value of each single measurement, $\Box_{A_i}\,(s_6^0 \wedge s_1^1 \wedge s_2^1 \wedge s_3^0)$.
- The dealer knows that the players know his bit and the players know that the dealer knows the sum of their bits, $\Box_D \Box_{A_i}\, s_6^0$ and $\Box_{A_i} \Box_D (s_1^{b_1} \oplus s_2^{b_2} \oplus s_3^{b_3})$.
- The adversary does not know any of the above, that is $\neg\Box_E\,(s_6^0 \wedge (s_1^{b_1} \oplus s_2^{b_2} \oplus s_3^{b_3}))$.
- The dealer and the agents know the above $\Box_\sigma \neg\Box_E\,(s_6^0 \wedge (s_1^{b_1} \oplus s_2^{b_2} \oplus s_3^{b_3}))$.

(ii) **Adversary's heaven**

The quantum channel is not safe and by rule (*iv*) we break its broadcasts to separate send and receive actions, whose appearances are not identities any

more. The appearances for a new qbit q_j with $j \geq 7$ are

$$f_{\sigma'}(\mathsf{qc}!^D q_i) = \begin{cases} \mathsf{qc}!^D q_i; \mathsf{qc}?^E q_i; P_i^{E,e}; N_j^{E,e}; \mathsf{qc}!^E q_j & \sigma' = E \\ \mathsf{qc}!^D q_j & o.w. \end{cases}$$

For the corresponding receive action, it appears to the dealer that players receive the qbit he sent to them, $f_D(\mathsf{qc}?^{A_i} q_i) = \mathsf{qc}?^{A_i} q_i$, whereas in reality they receive the qubit sent to them by adversary, $f_{A_i}(\mathsf{qc}?^{A_i} q_i) = \mathsf{qc}?^{A_i} q_j$. In case the eavesdropper is lucky and chooses the right projection for all three qubits he intercepts, he is able to derive the value of the key. In this case some of the epistemic properties of interest are

- The adversary knows the shared key, that is $\Box_E s_6^0$.
- The players and the dealer wrongly think that he does not know this $\Box_\sigma \neg \Box_E s_6^0$.
- Note that here the adversary has to be more lucky than in Ekert'91. This is because he has to intercept the qubits of three allied players instead of one, and has to choose from three measurement bases.

(iii) **Adversary's hell**

This is the same as above, but the players suspect adversary's actions, that is

$$f_{A_i}(\mathsf{qc}!^D q_i) = \mathsf{qc}!^D q_j \vee (\mathsf{qc}!^D q_i; \mathsf{qc}?^E q_i; P_i^{E,e}; N_j^{E,e}; \mathsf{qc}!^E q_j)$$

Similarly, the dealer suspect adversary's actions on the receipt of his sent qbit

$$f_D(\mathsf{qc}?^{A_i} q_i) = \mathsf{qc}?^{A_i} q_i \vee (\mathsf{qc}?^E q_i; P_i^{E,e}; N_j^{E,e}; \mathsf{qc}!^E q_j; \mathsf{qc}?^{A_i} q_j)$$

An interesting epistemic property is

The dealer and the players are not sure anymore if the adversary knows his bit $\neg \Box_\sigma \neg \Box_E s_6^0$.

We verify the property $\otimes_{i=1}^6 q_i \vdash [\pi] \Box_D \Box_i s_6^0$ in the agents' heaven and a similar one with $\neg \Box_\sigma \neg \Box_E s_6^0$. in the adversary's hell. The atomic expressions are generated via the following rewritings, where α_i's denote the juxtaposed actions of π,

$$\otimes_{i=1}^6 q_i \vdash [\pi] \Box_D \Box_{A_i} s_6^0 \quad \rightsquigarrow \quad \otimes_{i=1}^6 q_i; \pi \vdash \Box_D \Box_{A_i} s_6^0 \quad \rightsquigarrow \quad f_{A_i} f_D(\otimes_{i=1}^6 q_i; \pi) \vdash s_6^0 \rightsquigarrow$$
$$f_{A_i} f_D(\otimes_{i=1}^6 q_i); f_{A_i} f_D(\pi) \vdash s_6^0 \quad \rightsquigarrow \quad f_{A_i} f_D(\otimes_{i=1}^6 q_i); f_{A_i} f_D(\alpha_1); \cdots; f_{A_i} f_D(\alpha_n) \vdash s_6^0 \quad .$$

By rule (ii) of appearances we have $f_{A_i} f_D(\otimes_{i=1}^6 q_i) = \otimes_{i=1}^6 q_i$. By rule (iv) and our assumptions on channels, we have $f_D(\alpha_i) = \alpha_i$ for α_{A_i} a quantum or broadcast communication action. By rule (iii) for communication between players we have $f_D(\mathsf{c}!?_\beta^{A_i} s_i^j) = \mathsf{c}!?_\beta^{A_i} s_i^j \vee \mathsf{c}!?_\beta^{A_i} s_{\bar{i}}^j$, similarly for the projection actions

$$f_D(P_6^{D,+Z}) = P_6^{D,+Z}, \qquad f_D(P_1^{A_1,-Z}) = P_1^{A_1,-Z} \vee P_1^{A_1,+Z} \vee P_1^{A_1,-X} \vee P_1^{A_1,+X} \vee P_1^{A_1,-Y} \vee P_1^{A_1,+Y} \quad .$$

The values for the f_{A_i}'s are similarly set. Substituting these values in the above expression, we first eliminate the traces in which the bases of projections do not match the announced bases. Next we eliminate the communication actions from these traces whose content do not match the projections. As a result, we obtain a set of atomic expressions, of which only those satisfying $s_6^0 = s_1^{b_1} \oplus s_2^{b_2} \oplus s_3^{b_3}$ are well-defined in DMC. An example (out of four) is

$$\otimes_{i=1}^6 q_i; N_1; \ldots; N_6; \prod_{e_{ij}} E_{ij}; P_6^{D,+Z}; P_1^{A_1,+Z}; P_2^{A_2,-X}; P_3^{A_3,-Z} \vdash s_6^0 \quad .$$

This atomic expression is true, since in all its final configurations s_6 is 0, and thus our epistemic property holds for the secret sharing protocol. On the contrary, in the adversary's hell, one can similarly show that the epistemic property $\Box_D \neg \Box_E s_6^0$ does not hold and thus s_6^0 is not treated a secret anymore. Moreover, we also discover paths of an intercept-change attack for each agent, for example the one for the player A_1 contains the following sequence of actions

$$\cdots ; \mathtt{qc}!^D q_1; \mathtt{qc}?^E q_1; P_1^{E,+Z}; N_7^{E,+Z}; \mathtt{qc}!^E q_7; \mathtt{qc}?^{A_1} q_7; P_7^{A_1,+Z}; \cdots$$

4 Conclusion

In this article we proposed a new framework for formal analysis of security issues in quantum cryptographic protocols. The approach combines an algebraic rewrite system with a specification language for quantum distributed computations. The former provides machinery to work with uncertainties of agents in a protocol in a compositional way, while the latter inherently encodes the rules of quantum mechanics. Our framework was put to the test in the analysis of quantum secret sharing, where we showed some epistemic properties of the protocol in the presence and absence of an active adversary. As a procedure of this type typically becomes hairy, we envision providing a software implementation which automates the analysis of protocols. A software implementation of the algebra [15] is already in place to handle part of the verification. The construction of a tool that automatically derives the traces and semantics of a protocol is currently underway.

Acknowledgement

We had fruitful discussions with V. Danos, P. Panangaden, D. Markham. The second author has given talks on a version of the algebra with some quantum axioms encoded in it, which was partly based on joint work with E. Kashefi.

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.

[3] C.H. Bennett and G. Brassard, 'Quantum cryptography: public key distribution and coin tossing', in *Proceedings of IEEE international Conference on Computers, Systems and Signal Processing*, Bangalore, India, page 175. IEEE Press, 1984.

[4] B. Coecke and D. J. Moore and I. Stubbe, 'Quantaloids describing causation and propagation of physical properties', *Foundations of Physics Letters*, **14**, 2001.

[5] V. Danos, E. D'Hondt, E. Kashefi, and P. Panangaden, 'Distributed measurement-based quantum computation', in *Proceedings of the 3rd Workshop on Quantum Programming Languages (QPL05)*, ed. P. Selinger, 2005.

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

[7] V. Danos and E. D'Hondt, 'Quantum knowledge for cryptographic reasoning', in *Proc. 3rd International Workshop on Development of Computational Models (DCM07)*, ENTCS (to appear), 2008.

[8] E. D'Hondt and P. Panangaden, 'Reasoning about quantum knowledge', in *Proceedings of the 25th Conference on Foundations of Software Technology and Theoretical Computer Science*, LNCS vol. 382, page 0544c , 2006.

[9] A. K. Ekert, 'Quantum cryptography based on Bell's theorem', *Phys. Rev. Lett.*, 67(6):661–663, 1991.

[10] R. Fagin, J. Y. Halpern, Y. Moses and M. Y. Vardi. *Reasoning about Knowledge*. MIT Press, 1995.

[11] Simon J. Gay, Rajagopal Nagarajan and Nikolaos Papanikolaou, 'Probabilistic model-checking of quantum protocols', quant-ph/0504007, 2005.

[12] D. Markham, A. Roy and B. Sanders, 'Graph States for Quantum Secret Sharing', private communication, 2008.

[13] M.A. Nielsen and I. Chuang,*Quantum computation and quantum information*, Cambridge university press, 2000.

[14] P. Panangaden and K. Taylor, 'Concurrent Common Knowledge: Defining Agreement for Asynchronous Systems', *Journal of Distributed Computing* **6**, 1992.

[15] S. Richards and M. Sadrzadeh, '`Aximo`: Automated Axiomatic Reasoning for Information Update', *Proceedings of the 5th workshop on Methods for Modal Logic*, École normal supérieure de Cachan, Nov 2007, to appear in *Electronic Notes in Theoretical Computer Science*.

[16] M. Sadrzadeh, 'High-Level Quantum Structures in Linguistics and Multi-Agent Systems', AAAI Press, Proceedings of AAAI Spring Symposium on Quantum Interaction, 2007.

[17] M. Sadrzadeh, 'Actions and Resources in Epistemic Logic', Ph.D. Thesis, University of Quebec at Montreal, 2005, `http://eprints.ecs.soton.ac.uk/12823/01/all.pdf`.

[18] L. Xiao, G. Gong, F-G. Deng, and J-W. Pan. 'Efficient multiparty quantum-secret-sharing schemes', Phys. Rev. A, 69.