Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in Theoretical Computer Science

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