Journal of Symbolic Computation 73 (2016) 192–220

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Semi-automated verification of security proofs of quantum cryptographic protocols ☆

Takahiro Kubota [a,1], Yoshihiko Kakutani [a], Go Kato [b], Yasuhito Kawano [b], Hideki Sakurada [b]

[a] *Department of Computer Science, Graduate School of Information Science and Technology, University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo, 113-8656, Japan*
[b] *NTT Communication Science Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi-shi, Kanagawa, 243-0198, Japan*

ARTICLE INFO

Article history:
Received 27 February 2015
Accepted 10 May 2015
Available online 12 June 2015

Keywords:
Semi-automated verification
Quantum key distribution
Quantum protocols
Process calculi
Formal methods

ABSTRACT

This paper presents a formal framework for semi-automated verification of security proofs of quantum cryptographic protocols. We simplify the syntax and operational semantics of quantum process calculus qCCS so that verification of weak bisimilarity of configurations becomes easier. In addition, we generalize qCCS to handle security parameters and quantum states symbolically. We then prove the soundness of the proposed framework. A software tool, named the verifier, is implemented and applied to the verification of Shor and Preskill's unconditional security proof of BB84. As a result, we succeed in verifying the main part in Shor and Preskill's unconditional security proof of BB84 against an unlimited adversary's attack semi-automatically, i.e., it is automatic except for giving user-defined equations.

☆ A preliminary version of this paper was published in the Proceedings of Symbolic Computation in Software Science (SCSS 2013), RISC-Linz Report Series No. 13-06, pp. 64–69, Castle of Hagenberg, Austria (July 5–6, 2013).

E-mail addresses: takahiro.k11_30@is.s.u-tokyo.ac.jp (T. Kubota), kakutani@is.s.u-tokyo.ac.jp (Y. Kakutani), kato.go@lab.ntt.co.jp (G. Kato), kawano.yasuhito@lab.ntt.co.jp (Y. Kawano), sakurada.hideki@lab.ntt.co.jp (H. Sakurada).

[1] Takahiro Kubota's current affiliation is Toshiba Corporation.

http://dx.doi.org/10.1016/j.jsc.2015.05.001
0747-7171/

1. Introduction

Cryptographic protocols are essential elements of the infrastructure for ensuring secure communication and information processing. However, security proofs of such protocols tend to be complex and difficult to verify, which has been recognized by researchers (Shoup, 2004; Halevi, 2005). Indeed, flaws in designs (Lowe, 1996) and security proofs (Shoup, 2001; Galindo, 2005) of cryptographic protocols were found years after they had been presented. Formal methods have been applied to model, analyze, and verify cryptographic protocols. They are based on formal frameworks, including formal languages and inference rules to prove security properties. The languages are used to formalize cryptographic protocols and security properties, and the inference rules are used to perform formal proofs. Advantages of formal methods are as follows. First, the use of formal languages precisely prevents ambiguity. Although mathematical proofs in natural languages are rigorous, ones in formal languages can be more rigorous in terms of both description and interpretation, because their syntax and semantics are defined mathematically. Second, all inferences in a proof obey pre-defined inference rules. Third, verification can be automated, which reduces human costs and prevents errors.

Security proofs of quantum cryptographic protocols can be complex and difficult to verify because we must additionally consider attacks using entanglements. The first security proof of the BB84 quantum key distribution (QKD) protocol was presented by Mayers (2001). It is about 50 pages long and complex. Shor and Preskill presented a simple proof of BB84 (Shor and Preskill, 2000). They showed that the security of BB84 is equivalent to that of another QKD protocol based on entanglement distillation (the EDP-based protocol), whose security proof is simpler.

QKD protocols allow two remote principals to share a secret key using classical and quantum communication. Let us call the two principals Alice and Bob and the adversary Eve. An advantage of QKD protocols is that they do not depend on conjectured difficulty of computing certain functions, while the security of classical key exchange protocols is ensured on the basis of the difficulty (Diffie and Hellman, 1976). Moreover, QKD is one of the applications closest to practice in the quantum information field. Actually, several companies, such as Id Quantique, MagiQtechnologies, Toshiba, and NEC, are developing commercial quantum cryptographic systems. It is also possible that more complex quantum protocols will be presented in the future. Therefore, it is important to develop formal frameworks to verify quantum protocols' security and also make the security proofs machine-checkable.

Process calculi (Milner, 1999) are formal frameworks that are suitable to verify properties of parallel systems. They have been successfully applied to the verification of a number of classical cryptographic protocols such as Kerberos (Blanchet et al., 2008), which is a commercial authentication protocol. To clone the success in quantum information fields, several quantum process calculi, such as CQP (Nagarajan et al., 2005), qCCS (Lalire, 2006; Feng et al., 2007, 2011, 2012; Ying et al., 2009; Deng and Feng, 2012), and (Adão and Mateus, 2007), have been proposed. In qCCS, a quantum protocol is formalized as configuration $\langle P, \rho\rangle$, which is a pair comprising process P and quantum mixed state ρ that is referred to by using variables in P.

An important notion in process calculi is a *weak bisimulation* relation on processes (Milner, 1999; Feng et al., 2011; Deng and Feng, 2012). Processes in a weak bisimulation relation behave equivalently: they perform identical actions that are visible from the outside up to invisible ones. For example, visible actions are communications of processes via public channels, and invisible ones are communications via private channels. An example of usages of the relation is as follows. If we formalize some protocol and its specification as processes and prove that they are in a bisimulation relation, then we have proved the protocol satisfies the specification. Although there is a limitation regarding complexity of computation in this approach, as a great benefit, the conclusion is rigorously correct with absolute certainty.

In qCCS, the weak bisimulation relation $\approx$ on configurations is defined. The relation is closed by the application of parallel composition of processes: if $\langle P, \rho\rangle \approx \langle Q, \sigma\rangle$ holds, then $\langle P||R, \rho\rangle \approx \langle Q||R, \sigma\rangle$ holds for every process R with which $P||R$ and $Q||R$ are defined. $P||R$ means that P and R run in parallel. This property of $\approx$ is called congruence. Similarly in CQP, the weak bisimulation relation is defined and proved to be congruent. The congruence property is significant because we must take into account compositional behavioral equivalence.