Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Using quantum key distribution for cryptographic purposes: A survey [☆]

R. Alléaume [a,b,*], C. Branciard [c], J. Bouda [d], T. Debuisschert [e], M. Dianati [f], N. Gisin [c], M. Godfrey [g], P. Grangier [h], T. Länger [i], N. Lütkenhaus [j], C. Monyk [i], P. Painchault [k], M. Peev [i], A. Poppe [i], T. Pornin [l], J. Rarity [g], R. Renner [m], G. Ribordy [n], M. Riguidel [a], L. Salvail [o], A. Shields [p], H. Weinfurter [q], A. Zeilinger [r]

[a] *Telecom ParisTech & CNRS LTCI, Paris, France*
[b] *SeQureNet SARL, Paris, France*
[c] *University of Geneva, Switzerland*
[d] *Masaryk University, Brno, Czech Republic*
[e] *Thales Research and Technology, Orsay, France*
[f] *University of Surrey, Guildford, United Kingdom*
[g] *University of Bristol, United Kingdom*
[h] *CNRS, Institut d'Optique, Palaiseau, France*
[i] *Austrian Research Center, Vienna, Austria*
[j] *Institute for Quantum Computing, Waterloo, Canada*
[k] *Thales Communications, Colombes, France*
[l] *Cryptolog International, Paris, France*
[m] *Eidgenössische Technische Hochschule Zürich, Switzerland*
[n] *Id Quantique SA, Geneva, Switzerland*
[o] *Université de Montréal, Canada*
[p] *Toshiba Research Europe Ltd, Cambridge, United Kingdom*
[q] *Ludwig-Maximilians-University Munich, Germany*
[r] *University of Vienna, Austria*

ARTICLE INFO

Article history:
Received 1 April 2009
Accepted 1 August 2013
Available online xxxx

Keywords:
Key distribution
Quantum cryptography

ABSTRACT

The appealing feature of quantum key distribution (QKD), from a cryptographic viewpoint, is the ability to prove the information-theoretic security (ITS) of the established keys. As a key establishment primitive, QKD however does not provide a standalone security service in its own: the secret keys established by QKD are in general then used by a subsequent cryptographic applications for which the requirements, the context of use and the security properties can vary. It is therefore important, in the perspective of integrating QKD in security infrastructures, to analyze how QKD can be combined with other cryptographic primitives. The purpose of this survey article, which is mostly centered on European research results, is to contribute to such an analysis. We first review and compare the properties of the existing key establishment techniques, QKD being one of them. We then study more specifically two generic scenarios related to the practical use of QKD in cryptographic infrastructures: 1) using QKD as a key renewal technique for a symmetric cipher over a point-to-point link; 2) using QKD in a network containing many users with the objective of offering any-to-any key establishment service. We discuss the constraints as well as the potential interest of using QKD in these contexts. We finally give an overview

[☆] This document is the fruit of a collaborative effort initiated within the FP6 Trust and Security European integrated project SECOQC (IST-2002-506813). It is based for a large part on the SECOQC Crypto White Paper [1] that had been released in 2007.

[*] Corresponding author at: Telecom ParisTech & CNRS LTCI, Paris, France.
E-mail address: romain.alleaume@telecom-paristech.fr (R. Alléaume).

http://dx.doi.org/10.1016/j.tcs.2014.09.018

of challenges relative to the development of QKD technology that also constitute potential avenues for cryptographic research.

1. Introduction

In recent years quantum cryptography has been the subject of strong activity and rapid progress [2–4], and it is now extending its activity to pre-competitive research [5] and to commercial products [6]. Nevertheless, the fact that quantum key distribution (QKD) can play a useful role in practical cryptography is sometimes considered with skepticism [7–10] and cannot therefore been taken for granted. Analyzing the practical cryptographic implications of QKD is indeed a complex task that requires a combination of knowledge that usually belongs to separate academic communities, ranging from classical cryptography to the foundations of quantum mechanics and network security. Little work has so far been published on this issue, although [11] may be considered as a pioneering contribution on that matter. This review article tries to identify in which contexts QKD can be useful, in addition to the scientifically well-established classical cryptographic primitives.

The logical construction in the next three sections of this paper is to analyze the use of QKD, as a cryptographic primitive, for different purposes, reflecting the first three layers of the OSI network model.

1. Secret key agreement (performed in the case of QKD at the physical layer).
2. Secure payload transmission built on top of a key agreement scheme (secure link layer cryptographic primitive).
3. Secret key agreement over a global network composed of multiple users (network layer cryptographic primitive).

The paper is thus organized as follows: In Section 2, we provide a survey of secret key agreement techniques and discuss some of their strengths, weaknesses, and relative advantages. In Section 3, we discuss the security and the performance of different secure payload transmission primitives that can be built on top of QKD, and that can be used to secure point-to-point communication links. In Section 4, we consider the use of QKD in a network context. We discuss previous works on QKD networks and also describe the cryptographic operation of such networks and in particular their initialization, that requires the distribution of pre-shared secrets. Finally, in Section 5 we widen the scope of this survey paper by discussing some future research directions that could benefit from active collaboration between the quantum and the classical cryptography communities: the study of side-channels and of material security, the study of post-quantum-computing cryptography, the use of QKD networks as a strong building block for new network security protocols and the development of unified cryptographic standards and evaluation methods for quantum and classical cryptography.

2. Secret key agreement

Cryptography has for a long time conformed to the idea that the techniques used to protect sensitive data had themselves to be kept secret. Such principle, known as "cryptography by obscurity" has however become inadequate in our modern era. The cryptography that has developed as a science in the 1970s and 1980s [12] has allowed us to move away from this historical picture and most of the modern cryptographic systems are now based on publicly announced algorithms while their security lies in the use of secret keys.

Distributing keys among a set of legitimate users while guaranteeing the secrecy of these keys with respect to any potential opponent is thus a central issue in cryptography, known as the *secret key agreement problem*.

There are currently five families of cryptographic methods that can be used to solve the secret key agreement problem between distant users:

1. Classical ITS schemes
2. Classical computationally secure public-key cryptography
3. Classical computationally secure symmetric-key cryptographic schemes
4. Quantum key distribution
5. Trusted couriers

We will present how each of these cryptographic families can provide solutions to the key agreement problem and discuss, in each case, the type of security that can be provided. We will also consider a sixth type of secret key agreement schemes: hybrid schemes built by combining some of the methods listed above.

2.1. Classical information-theoretically secure key agreement schemes

A cryptosystem is information-theoretically secure (ITS) if its security derives purely from information theory. That is, it makes no unproven assumptions on the hardness of some mathematical problems, and is hence secure even when the ad-

Please cite this article in press as: R. Alléaume et al., Using quantum key distribution for cryptographic purposes: A survey, Theor. Comput. Sci. (2014), http://dx.doi.org/10.1016/j.tcs.2014.09.018