Theoretical Computer Science ••• (••••) •••–•••

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Public-key cryptography based on bounded quantum reference frames

Lawrence M. Ioannou [a,*], Michele Mosca [a,b]

[a] Institute for Quantum Computing and Department of Combinatorics and Optimization, University of Waterloo, 200 University Avenue, Waterloo, Ontario, N2L 3G1, Canada
[b] Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, Ontario, N2L 2Y5, Canada

ARTICLE INFO

Article history:
Received 2 March 2009
Accepted 31 May 2011
Available online xxxx

Keywords:
Public-key authentication
Identification
Quantum-public-key cryptography
Reference frames

ABSTRACT

We demonstrate that the framework of bounded quantum reference frames has application to building quantum-public-key cryptographic protocols and proving their security. Thus, the framework we introduce can be seen as a public-key analogue of the framework of Bartlett et al. [1], where a private shared reference frame is shown to have cryptographic application. The protocol we present in this paper is an identification scheme, which, like a digital signature scheme, is a type of authentication scheme. We prove that our protocol is both reusable and secure under the honest-verifier assumption. Thus, we also demonstrate that secure reusable quantum-public-key authentication is possible to some extent.

1. Introduction

Since its inception, the focus of quantum cryptography has been on the symmetric-key model, where Alice and Bob attempt to generate private shared correlations (as in quantum key distribution [2,3]) or are assumed to hold them (as in quantum authentication [4]). Such correlations can usually be defined or encoded by a string of bits—the secret key—but Bartlett et al. [1] showed that they may also take the form of a private shared reference frame. Symmetric-key quantum protocols are usually unconditionally secure, meaning that the sole assumption is that (some part of) quantum theory is correct; however, Damgaard et al. [5,6] have investigated information-theoretically secure protocols, such as password-based identification and bit commitment, in the bounded quantum storage model, where an extra assumption is that the size or quality of the adversary's quantum memory is limited (see also Refs. [7–9]).[1]

Going beyond the symmetric-key model, but retaining unconditional security, Gottesman and Chuang [11] introduced quantum-public-key cryptography—where the public keys are quantum systems, each of whose state encodes the (same) classical private key—by giving a secure one-time (digital) signature scheme for signing classical messages.

A public-key framework eliminates the need for Alice and Bob to establish private shared correlations, which has practical advantages in large networks of users (where there may be many "Alices" or "Bobs"). Alice chooses a random private key, creates copies of the corresponding public key, and distributes the copies in an authenticated fashion to all potential "Bobs". In principle, this asymmetric setup allows, e.g., any Bob to send encrypted messages to Alice or to verify any signature for a message that Alice digitally signed, thus significantly reducing the number of secret/private keys involved as compared to

* Corresponding author.
E-mail addresses: lmioannou@gmail.com (L.M. Ioannou), mmosca@iqc.ca (M. Mosca).

[1] The bounded storage model for classical protocols (e.g. Ref. [10]), where the adversary's classical memory is assumed to be bounded, also gives information-theoretic security.

http://dx.doi.org/10.1016/j.tcs.2014.09.016
0304-3975/

the case where each Alice–Bob pair shares a secret key and uses symmetric-key protocols. Thus the public-key framework vastly simplifies key distribution, which is often the most costly part of any cryptosystem. Note that the security of classical public-key protocols is necessarily based on computational assumptions [12].

The mapping that takes a private key to the state of the corresponding quantum public key is always assumed to be publicly known. Furthermore, in any reasonable quantum-public-key system, the states of two quantum public keys corresponding to two different private keys always have overlap less than $(1-\delta)$, for some positive and publicly known δ. Thus, a striking aspect of quantum-public-key cryptography that sets it apart from its classical counterpart is that the number of copies of the (quantum) public key in circulation must be limited. If this were not the case, then an adversary could collect an arbitrarily large number of copies, measure them all, and determine the private key.

The limit on the number of copies of the quantum public key implies that not everyone can use the protocol; however, in practice, the maximum number of users (or uses) of any particular protocol can be estimated, and thus the parameters of the protocol can be adjusted so that the limit allows for this maximum. Increasing this limit would presumably result in a less efficient instance of the protocol, and this is one kind of tradeoff between efficiency and usability in the quantum-public-key setting. Another kind concerns reusability. For instance, the abovementioned signature scheme is "one-time" because only one message may be signed under a particular key-value, even though many different users can verify that one signature. If a second message needs to be signed, the signer must choose a new private key and then distribute corresponding new public keys. One open problem is thus whether there exist reusable signature schemes, where either the same copy of the public key can be used to verify many different message-signature pairs securely, or where just the same key-values can be used to verify many different message-signature pairs securely (but a fresh copy of the public key is needed for each verification). The latter notion of "reusability" is what we adopt here.

What makes a key *public*? In principle, Alice's public-key-generation algorithm, which takes as input the private key and outputs one copy of the quantum public key, may output a system in a pure state or a mixed state, from Alice's point of view (a mixed state is a fixed probabilistic distribution of pure states). In the original framework of Gottesman and Chuang, the algorithm is assumed to produce a system in a pure state. For some applications, like digital signature schemes, this purity is crucial; for, otherwise, Alice could cheat by sending different public keys to different "Bobs". Purity prevents Alice's cheating here because different "Bobs" can compare their copies of the public key via a "distributed SWAP-test" [11] to see if they are the same (with high probability), much like can be done in the case of classical public keys. But the ability to do an equality test benefits any scheme, since an adversary who tries to substitute bad keys for legitimate ones could thus be caught. Indeed, if the public-key-generation algorithm produces a mixed state, since there is no equality test guaranteed to recognize when two mixed states are equal, then no such test for equality of public keys may be possible—this is at odds with what it means to be "public", i.e., publicly verifiable.[2] While the scheme we present in this paper does not explicitly make use of the "distributed SWAP-test" (since we assume the public keys have been distributed securely), it can do so in principle. We view this as analogous to how modern public-key protocols do not explicitly specify an equality test among unsure "Bobs", but how the framework naturally allows such a test which would thwart attempts to distribute fake public keys.

Our work appears to be of a dramatically different character when compared to other explorations of quantum-public-key protocols [13–17]: we demonstrate that the framework of bounded quantum reference frames [18] has application to building such protocols and proving their security. Thus, the framework we introduce can be seen as a public-key analogue of the framework of Bartlett et al. [1].

We stress that our work in public-key quantum cryptography strives for unconditional security, as opposed to security based on computational assumptions [12]. In particular, our work is unrelated to the work in Ref. [19], where classical public-key systems (whose security must be based on computational assumptions) are constructed that require a quantum computer for the generation of the public keys.

The protocol we present in this paper is an identification scheme, which, like a digital signature scheme, is a type of authentication scheme. Authentication schemes are not concerned with ensuring the *privacy* of information, but rather seek to ensure its *integrity*. For example, digital signature schemes (and message authentication codes) ensure the integrity of origin of messages, whereas identification schemes ensure the integrity of origin of communication in real time [12]. Identification protocols are said to ensure "aliveness"—that the entity proving its identity is active at the time the protocol is executed.

We prove that our identification protocol is both reusable and secure under the honest-verifier assumption (defined in the next section). Thus, we also demonstrate that secure reusable quantum-public-key authentication is possible to some extent.

We now proceed with a description of our protocol (Section 2) and the honest-verifier security proof (Section 3).

[2] Other authors have defined the framework to include mixed public keys, and Ref. [13] proposes an encryption scheme with mixed public keys that is reusable and unconditionally secure [14].

Please cite this article in press as: L.M. Ioannou, M. Mosca, Public-key cryptography based on bounded quantum reference frames, Theor. Comput. Sci. (2014), http://dx.doi.org/10.1016/j.tcs.2014.09.016