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

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Secure identification and QKD in the bounded-quantum-storage model ☆

Ivan Damgård [a], Serge Fehr [b,*], Louis Salvail [c], Christian Schaffner [d,b]

[a] Department of Computer Science, Aarhus University, Denmark
[b] CWI Amsterdam, The Netherlands
[c] Université de Montréal (DIRO), QC, Canada
[d] ILLC, University of Amsterdam, The Netherlands

ARTICLE INFO

Article history:
Received 22 July 2009
Accepted 16 May 2014
Available online xxxx

Keywords:
Quantum cryptography
Bounded-quantum-storage model

ABSTRACT

We consider the problem of secure identification: user U proves to server S that he knows an agreed (possibly low-entropy) password w, while giving away as little information on w as possible—the adversary can exclude at most one possible password for each execution. We propose a solution in the bounded-quantum-storage model, where U and S may exchange qubits, and a dishonest party is assumed to have limited quantum memory. No other restriction is posed upon the adversary. An improved version of the proposed identification scheme is also secure against a man-in-the-middle attack, but requires U and S to additionally share a high-entropy key k. However, security is still guaranteed if one party loses k to the attacker but notices the loss. In both versions, the honest participants need no quantum memory, and noise and imperfect quantum sources can be tolerated. The schemes compose sequentially, and w and k can securely be re-used. A small modification to the identification scheme results in a quantum-key-distribution (QKD) scheme, secure in the bounded-quantum-storage model, with the same re-usability properties of the keys, and without assuming authenticated channels. This is in sharp contrast to known QKD schemes (with unbounded adversary) without authenticated channels, where authentication keys must be updated, and unsuccessful executions can cause the parties to run out of keys.

1. Introduction

Secure identification Consider two parties, a *user* U and a *server* S, who share a common secret-key (or password or Personal Identification Number PIN) w. In order to obtain some service from S, U needs to convince S that he is the legitimate user U by "proving" that he knows w. In practice—think of how you prove to the ATM that you know your PIN—such a proof is often done simply by announcing w to S. This indeed guarantees that a dishonest user U* who does not know w cannot identify himself as U, but of course incurs the risk that U might reveal w to a malicious server S* who may now impersonate U. Thus, from a secure identification scheme we also require that a dishonest server S* obtains (essentially) no information on w.

☆ A preliminary version of this paper appeared in CRYPTO 2007.

* Corresponding author.
E-mail addresses: ivan@cs.au.dk (I. Damgård), fehr@cwi.nl (S. Fehr), salvail@iro.umontreal.ca (L. Salvail), c.schaffner@uva.nl (C. Schaffner).

http://dx.doi.org/10.1016/j.tcs.2014.09.014
0304-3975/

There exist various approaches to obtain secure identification schemes, depending on the setting and the exact security requirements. For instance zero-knowledge proofs (and some weaker versions), as initiated by Feige, Fiat and Shamir [19,18], allow for secure identification. In a more sophisticated model, where we allow the common key w to be of low entropy and additionally consider a man-in-the-middle attack, we can use techniques from password-based key-agreement (like [21, 20]) to obtain secure identification schemes. Common to these approaches is that security relies on the assumption that some computational problem (like factoring or computing discrete logs) is hard and that the attacker has limited computing power.

Our contribution In this work, we take a new approach: we consider quantum communication, and we develop two identification schemes which are information-theoretically secure under the *sole* assumption that the attacker can only reliably store quantum states of limited size. This model was first considered in [9]. On the other hand, the honest participants only need to send qubits and measure them immediately upon arrival, no quantum storage or quantum computation is required. Furthermore, our identification schemes are robust to both noisy quantum channels and imperfect quantum sources. Our schemes can therefore be implemented in practice using existing technology.

The first scheme is secure against dishonest users and servers but not against a man-in-the-middle attack. It allows the common secret-key w to be non-uniform and of low entropy, like a human-memorizable password. Only a user knowing w can succeed in convincing the server. In any execution of this scheme, a dishonest user or server cannot learn more on w than excluding one possibility, which is unavoidable. This is sometimes referred to as *password-based* identification. The second scheme requires in addition to w a uniformly distributed high-entropy common secret-key k, but is additionally secure against a man-in-the-middle attack. Furthermore, security against a dishonest user or server holds as for the first scheme even if the dishonest party knows k (but not w). This implies that k can for instance be stored on a smart card, and security of the scheme is still guaranteed even if the smart card gets stolen, assuming that the affected party notices the theft and thus does not engage in the scheme anymore. Both schemes compose sequentially, and w (and k) may be safely re-used super-polynomially many times, even if the identification fails (due to an attack, or due to a technical failure).

A small modification of the second identification scheme results in a quantum-key-distribution (QKD) scheme secure against bounded-quantum-memory adversaries. The advantage of the proposed new QKD scheme is that no authenticated channel is needed and the attacker can *not* force the parties to run out of authentication keys. The honest parties merely need to share a password w and a high-entropy secret-key k, which they can safely re-use (super-polynomially many times), independent of whether QKD succeeds or fails. Furthermore, like for the identification scheme, losing k does not compromise security as long as the loss is noticed by the corresponding party. One may think of this as a quantum version of password-based authenticated key exchange. The properties of our solution are in sharp contrast to all known QKD schemes without authenticated channels (which do not pose any restrictions on the attacker). In these schemes, an attacker can force parties to run out of authentication keys by making the QKD execution fail (e.g. by blocking some messages). Worse, even if the QKD execution fails only due to technical problems, the parties can still run out of authentication keys after a short while, since they cannot exclude that an eavesdropper was in fact present. This problem is an important drawback of QKD implementations, especially of those susceptible to single (or few) point(s) of failure [14].

Other approaches We briefly discuss how our identification schemes compare with other approaches. We have already given some indication on how to construct *computationally* secure identification schemes. This approach typically allows for very practical schemes, but requires some unproven complexity assumption. Another interesting difference between the two approaches: whereas for (known) computationally-secure password-based identification schemes the underlying computational hardness assumption needs to hold indefinitely, the restriction on the attacker's quantum memory in our approach only needs to hold *during* the execution of the identification scheme, actually only at one single point during the execution. In other words, having a super-quantum-storage-device at home in the basement only helps you cheat at the ATM if you can communicate with it on-line quantumly—in contrast to a computational solution, where an off-line super-computer in the basement can make a crucial difference.

Furthermore, obtaining a satisfactory identification scheme requires *some* restriction on the adversary, even in the quantum setting: considering only passive attacks, Lo [24] showed that for an unrestricted adversary, no password-based quantum identification scheme exists. Lo's impossibility result only applies if the user U is guaranteed not to learn anything about the outcome of the identification procedure. The impossibility of the general case has been shown in very recent work [4]. Using the definitions from [17], one can even show that the whole password of the honest player leaks to the dishonest player.

Another alternative approach is the classical bounded-storage model [25,5,1]. In contrast to our approach, only classical communication is used, and it is assumed that the attacker's *classical* memory is bounded. Unlike in the quantum case where we do not need to require the honest players to have any quantum memory, the classical bounded-storage model requires honest parties to have a certain amount of memory which is related to the allowed memory size of the adversary: if two legitimate users need n bits of memory in an identification protocol meeting our security criterion, then an adversary must be bounded in memory to $O(n^2)$ bits. The reason is that given a secure password-based identification scheme, one can construct (in a black-box manner) a key-distribution scheme that produces a one-bit key on which the adversary has an (average) entropy of $\frac{1}{2}$. On the other hand it is known that in any key-distribution scheme which requires n bits of memory for legitimate players, an adversary with memory $\Omega(n^2)$ can obtain the key except for an arbitrarily small

Please cite this article in press as: I. Damgård et al., Secure identification and QKD in the bounded-quantum-storage model, Theor. Comput. Sci. (2014), http://dx.doi.org/10.1016/j.tcs.2014.09.014