Blind signatures using offline repositories

May 13 2015

Digital signatures are mechanisms for authenticating the validity or authorship of a certain digital message and they aim to be digital counterparts to real (or analog) signatures. The concept was introduced by Diffie and Hellman in 1976. Notice that, when certified, digital signatures have the same legal power as traditional signatures.

With the advent of quantum computation new threats to security became a near future reality and all known digital signatures schemes are vulnerable, compromising fundamental properties of signature schemes: authenticity and authorship uniqueness. In order to overcome the potential threat of quantum computation, the community started to envisage the possibility of using quantum mechanics laws to develop new protocols that are resilient against quantum adversaries.

In the paper we show how to build such a digital blind signature scheme under the assumption that we have an offline repository and using quantum information. As a future work of this application would be the possibility of creating untraceable money, an ultimate goal of cryptography.

This work was partially supported, under the PQDR (Probabilistic, Quantum and Differential Reasoning) and Capri initiatives of SQIG at IT, CV-Quantum initiative of SQIG and Optical Communications and Photonics groups at IT, by FCT and EU FEDER, namely via the FCT PEst-OE/EEI/LA0008/2013 and UID/EEA/50008/ 2013 projects, as well as by the European Union's Seventh Framework Programme for Research (FP7). Andre Souto also acknowledges the FCT postdoc grant

SFRH/ BPD/76231/2011. Joao Ribeiro acknowledges the scholarship awarded by Fundacao Calouste Gulbenkian through the program Novos Talentos em Matematica for undergraduate students.

More information: The paper can be found in www.worldscientific.com/doi/pd … 42/S0219749915500161 in latest issue of the *International Journal of Quantum Information* (*IJQI*).