

عنوان مقاله:

A Weak Blind Signature Based on Quantum Key Distribution

محل انتشار:

مجله محاسبات و امنیت, دوره 1, شماره 3 (سال: 1393)

تعداد صفحات اصل مقاله: 8

نویسندگان:

Siavash Khodambashi - Faculty of Electrical and computer engineering, Shahid Beheshti University

Ali Zakerolhosseini - Assistant Professor, Faculty of Electrical and computer engineering, Shahid Beheshti University

خلاصه مقاله:

Recently, the laws of quantum physics have amazed classical cryptography and aided researchers to provide secure communications in presence of adversaries. In this paper we present a novel weak blind signature scheme whose security is guaranteed by fundamental principles of quantum physics. Despite previous schemes which are taking advantage of quantum entangled states, our proposed quantum blind signature relies only on Quantum Key Distribution (QKD) protocol. We show throughout this paper that our proposed quantum weak blind signature achieves a good position in security and reliability. In addition, it is feasible for the proposed scheme to become commercialized with current technology. Hence, it can be widely used for e-payment, e-government, e-business and etc.

کلمات کلیدی:

Quantum Weak Blind Signature, Quantum Key Distribution, Quantum Cryptography, Quantum Payment

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/1366334>

