NEW PHYSICAL ATTACKS AND SECURITY OF SMART-CARD

Jaroslav Hrubý
hruby@gcucmp.cz

Institute of Physics of Academy of Sciences of the Czech Republic,
Na Slovance 2, Prague 8, Czech Republic

Abstract

Power analysis is a successful cryptanalytic technique which extracts secret information from smart-cards by analysing the power consumed during the execution of their internal programs. The attack is particularly dangerous in financial application in which users inserts their smart-card into teller machine which are owned and operated by potentially dishonest entities.
In this paper we describe a new solution to the problem, which is based on an application of quantum cryptography with quantum entanglement for smart-cards.

Keywords: power analysis, quantum entanglement, identification, smart-card.

1. Introduction

An interesting application of quantum cryptography for smart-cards using quantum transmission of photons and an application of quantum key distribution for the quantum identification system were published [1]. Here we present a new application of quantum entanglement for smart-cards to eliminate the new physical attacks on the smart-card.

The necessity to look for more secure smart-cards follows as the consequence of the fault case presented in the New York Times headline [2] or new attacks via power and differential power analysis [3]. Kocher et al. have proposed these new physical attacks: simple power analysis, where the eavesdroper tries to recover information about the secret key by simple measuring the power consumption of the computing device, and the more complex differential power analysis additionally requires knowledge of ciphertext outputs and is thus more costly.

Generally we can summarize, that there are the following basic problems with existing identification systems using smart-cards:

1) the customer must type the PIN (Personal Identification Number) to an unknown teller machine which can be modified to memorize the PIN;
2) the customer must submit the smart-card with information needed for the identification to an unknown teller machine; in presence of an eavesdroper it can be also memorized together with the

PIN.
3) the smart-card based on silicon technology can be attacked even without its interaction with the teller machine via many noninvasive physical attacks.

In this way such identification system via smart-card can fail. The solution of these problems is to employ optical fibres and optoelectronics on the smart-card together with entangled quantum optical states.

Here we present a new identification system, which in principle can be based on quantum entanglement of two photons and which solves these basic problems in the following way:
1) PIN will be typed directly to the card for activation of the optoelectronics devices located on the smart-card and no PIN information will be exchanged with the teller machine.
2) The information needed for the identification of the card inside the teller machine will be protected against an eavesdropper through non-local projection of the state of one member of the pair of entangled photons which will happen during its propagation directly on the smart card.
3) The power source is put directly on the smart-card (e.g., a photocell).

It is well known that in the ordinary teller machine without quantum channels all carriers of information are physical objects open to copying or cloning. The information for the identification of the card is enclosed by modification of their physical properties. The laws of the classical theory allow the dishonest eavesdropper to measure and copy the cryptographic key information precisely.

This is not the case when the nature of the channels is such that quantum theory is needed for their description. Any totally passive or active eavesdropper operating on the quantum channel can be detected.

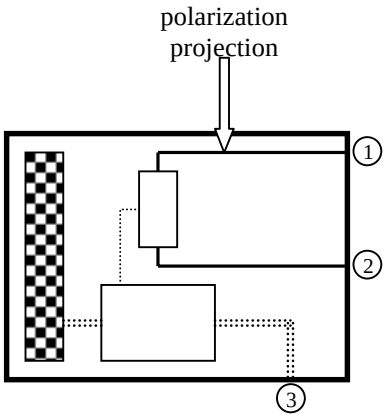
The current development of technologies of fiber and intergrated optics makes it possible to construct quantum optoelectronic smart-card for our application. The travelling distance for quantum transmission is very short here. This means, that the problems appearing in application of ordinary quantum cryptography in optical communications are negligible here.

The new idea presented here is, that the projection on a selected polarization basis of the entangled photon from the Einstein-Podolsky-Rosen (EPR) pair of polarized photons occurs directly inside the smart-card, at the moment when the second member of the pair is measured in the same basis inside the teller machine.

2. The quantum entanglement for the smart-card

A scheme of the QC smart-card with the quantum entanglement is given in Fig.1. Here the solid line presents the quantum channel (optical fiber), the double dotted line presents the electric connection from the photocell source and signal connection with teller machine. The single dotted line is the signal pulse connection between the microchip and polarization modulator, which are integrated and with active shielding are ”secure“ against external measurements of electromagnetic fields from signal pulses. An arrow indicates the position of the correlated photon on the smart-card at the instant of the measurement of the other member of the pair in the teller machine.

This quantum card consists of:



a) a PIN activator, which can have the form of the ordinary card light-source calculator with sensor keys; the user puts the PIN on the card to identify himself in a secure distance from the teller (i.e. unknown quantum cryptographic verification device) and in a secure outer area; the card will be blocked when the sequence of the three incorrect PINs will be given; as soon as the activated card is not used within short time period (say, 20 s), the activation is closed;
b) a microchip with the implemented cryptographic key $\{0,1\}^n$ which is long enough to yield required security for the given protocol; the microchip is activated when correct PIN is entered on the card;
c) a polarization modulator (PM), which transforms the cryptographic key $\{0,1\}^n$ to the optical polarization states of the photon under the following encoding rules:
   "0" is encoded as no change of the polarization;
   "1" is encoded as change of the polarization state to the other basis state.
d) a quantum channel consisting of a singlemode optical fiber.

The smart-card is equipped with the optical connectors ①,② for connecting the quantum channel to the teller machine and electric connector ③ that serves for auxiliary communication needed to trigger and synchronize the operation of the smart-card with the arrival of photons from the teller and possibly also for the exchange of classical information needed for realization of the cryptographic protocol.

Present technologies give the possibility to construct the card without significant radiation of electromagnetic energy and a new generation of microchips, which together with optoelectronics elements are resistant against possible known physical attacks. The main advantage is that no classical secret information ever leaves the smart-card, only quantum information is going out.

In this way the smart-card controls the polarization of the photon which was projected randomly at one of the two possible polarization states directly on the smart-card and no eavesdropper inside the card slot has a chance to read-out the authentication information without being detected.

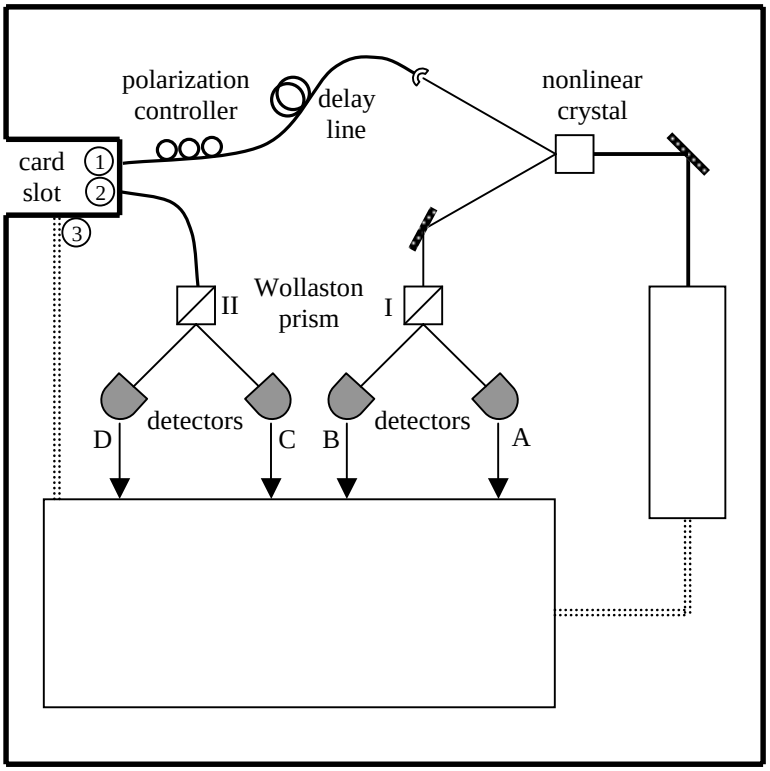
3.The teller machine with quantum entanglement

The teller machine, which is based on the quantum correlation principle, is plotted in Fig.2 and consists of :

i) source of EPR photons; a pulsed laser source can be used to pump the down-conversion process in a nonlinear crystal;
ii) the delay line that determines the moment of the projection of the polarization state of the correlated photon on the smart-card at the moment of the detection of the second member of the pair in the teller machine;
iii) the polarization controller serves for compensation of the polarization changes in the device,

iv) Wollaston prism I serves for random projection of the polarization of one of the photons while Wollaston prism II is used to analyze the resulting polarization state of the other photon;

v) the two pairs of photon-counting detectors are used to detect the outputs of the Wollaston prisms. The first pair of detectors (A,B) detects the realization of random projection in the Wollaston prism I for the photon that remains inside the teller machine. The second pair of detectors (C,D) is used to measure the state of the second EPR photon which is coming modified or not-modified from the smart-card. Via modification of the polarization smart-card sends its secret;



TELLER

vi) the computer that drives the operation of the whole device and where the information obtained by measurement on the detectors A,B,C,D is processed according to the given cryptographic protocol and the authentication key is compared to its stored replica;

vii) all quantum optical paths inside the teller machine can be done with ordinary optical single-mode fibers (solid line) and electric signal channel (dotted line) are in the same quality like on the smart-card.

In such realization the smart-card controls polarization while the teller machine controls detectors and can obtain the secret information from smart–card only via quantum transmission. The teller machine accepts or rejects the smart-card if the secret information coincides with the replica stored in its database up to a tolerable amount of errors. Some amount of errors must be tolerated due to physical imperfections of the device.

This is the authentication of the smart-card, which can be improved via known cryptographic protocols that combine sending the classical public information, which can be under eavesdropper's control, and quantum secret information, where eavesdropper's activity will be detected.

4. Conclusions

We have discussed the possibility to utilize the advantages of quantum correlation for authentication. Of course if we have more ”robust“ smart-card with detectors we can provide the mutual identification between smart-card and teller machine via quantum cryptography.

Manufactures should be encouraged to develop enough cheap photon-counting detectors and smaller optoelectronics elements integrating the new generation of microchips with polarization modulators.

We have shown a new positive solution to the open problem connected with the smart-card security.

Acknowledgement

This work was supported by grants RN19982003012, RN19982003013 and LN00A015 with subvention of the Ministry of Education of the Czech Republic. The author would like to thank Ondrej Haderka for stimulating discussions and helpful comments. The presentation is supported
by Hewlett - Packard s.r.o.

References

[1] Hrubý J.: *Smart-card with Interferometric Quantum cryptography device*, Lecture Notes in Computer Science 1029 (1995), p.282;
Dušek M., Haderka O., Hendrych M. and Myška R.: *Quantum identification system*, Phys. Rev A, v.60 ,n.1 (1999), p.149.

[2] *One Less Thing to Believe In: Fraud at Fake Cash Machine*, New York Times 13 May 1993, pp. A1 \& B9.

[3] Kocher P., Jaffe J. and Jun B.: *Differential Power Analysis*, Advances in Cryptology-Proceedings of CRYPTO`99, Lecture Notes in Computer Science, Vol.1666, Spriner-Verlag,(1999).