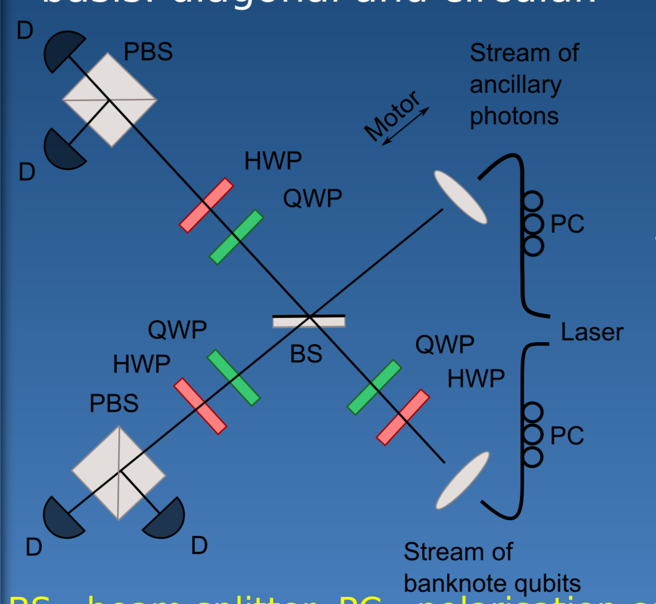
Experimental counterfeiting of quantum money

Kateřina Jiráková, Karol Bartkiewicz, Antonín Černoch, and Karel Lemr

Experimental Setup

The measurement has been held using the following setup. We cloned four polarisation states of single photons: D, A, R and L and analysed them in two basis: diagonal and circular.



The cloning was facilitated by an unbalanced beam splitter (BS) with splitting ratio 81/19 and 19/81 for horizontal and vertical polarisation, respectively. For generation of photon pairs we used spontaneous parametric down-conversion using BBO crystals. Qubits are encoded into the polarisation states of individual photons. States to be cloned are prepared in the lower arm and the upper arm is a source of ancillary photon. The cloning is successful only if each photon leaves BS by different output port, therefore we are interested in coincidences between both output arms.

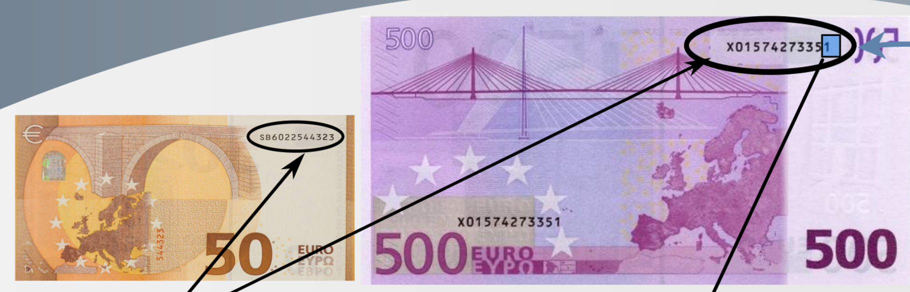
BS - beam splitter, PC - polarisation controler, HWP/QWP - half/quater wave plate, D - detector, PBS - polarisation beam splitter

Motivation

The concept of quantum money has been originally suggested by S. Wiesner [Wiesner1983]. It is advantageous because copying of quantum banknotes leaves the quantum states changed (mark of counterfeiting the money).

The quantum states cannot be in general perfectly cloned (no-cloning theorem), however, an imperfect cloning is still possible and provides us with a mean to an eavesdropping attack on the protocol proposed by Bozzio [Bozzio2018].

Scheme of the attack:



banknotes are composed of sequences of qubit pairs (8 combinations)

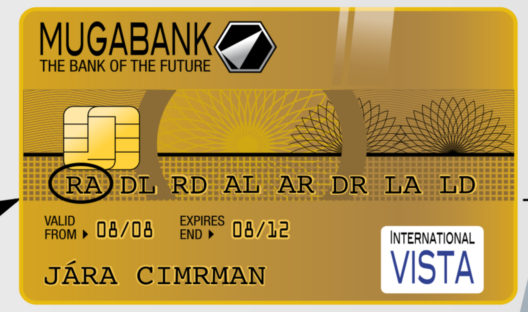
for convenience expressed in octal system

a credit card incorporates several quantum banknotes

each sequence is calculated from serial number (SN) using a secret function

|DR⟩	|AR⟩
|DL⟩	|AL⟩
|RD⟩	|RA⟩
|LD⟩	|LA⟩

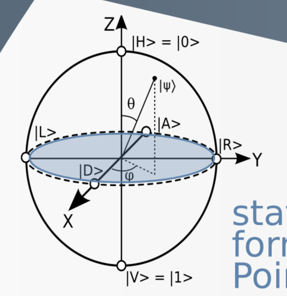
proposed in [Bozzio2018]



e. g. rotating cipher or hash function

payment

Legitimate terminal should extract states and perform measurement without cloning (attackers terminal clones)



states |L⟩, |R⟩, |D⟩ and |A⟩ form an equator of the Poincare sphere

By performing cloning the attacker gains some information about the encoding of currently used banknotes. This information can be later used to counterfeit so far unused banknotes because random generation of SN is not computationally feasible [Aaronson2012].

MULTIPHOTON QUANTUM LAB

multiphoton.upol.cz

RCPTM

Strategies of the attack

1. to provide bank with measurement outcome every time cloning takes place and if it fails, send a random value
2. to send measurement outcome, only if it is registered by the terminal and report a lost qubit when cloning fails
3. to measure qubits after their extraction from the credit card in given basis but do NOT perform cloning at all

extracting + clonning 1→2

optimal phase-covariant quantum cloning using an unbalanced beam splitter (splitting ratio 79/21) [Fiurasek2003]

clones: |RA⟩ |RA⟩

measuring in diagonal (D/A) or circular (R/L) basis

measurement basis requested by the bank

possible results:

the bank requested e. g. D/A basis

~~|DR⟩~~	~~|AR⟩~~
~~|DL⟩~~	~~|AL⟩~~
~~|RD⟩~~	|RA⟩
~~|LD⟩~~	|LA⟩

certain

|RA⟩	|LA⟩
|RA⟩	|LA⟩
|RA⟩	|LA⟩
|LA⟩	|RA⟩

random

no information gained |? ?⟩

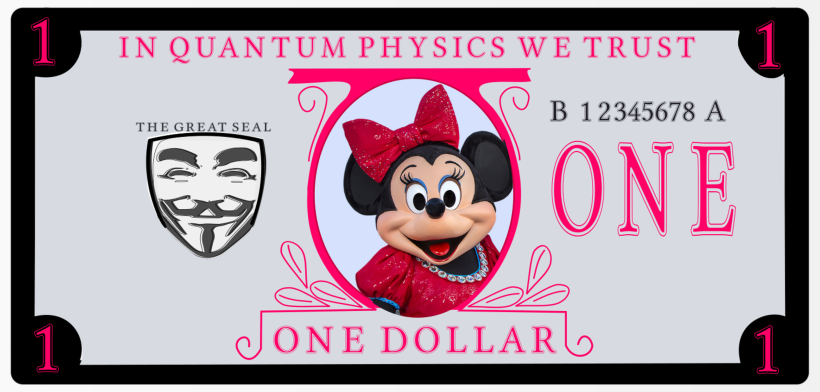
the attacker reveals the state of the second qubit

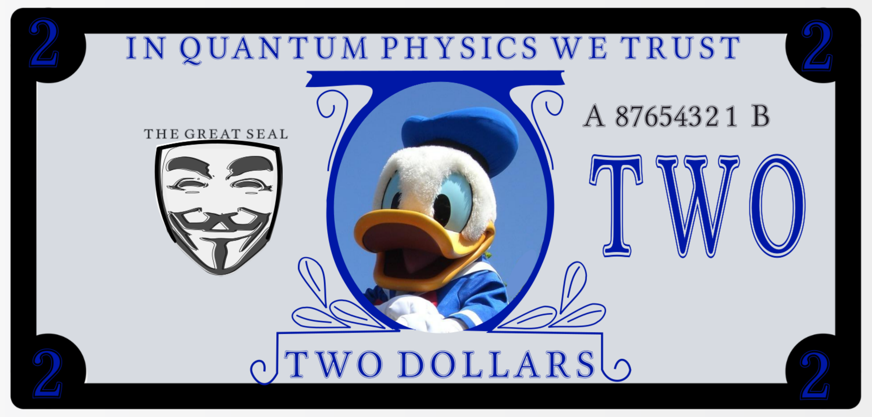
the attacker knows what encoding was used

information gained

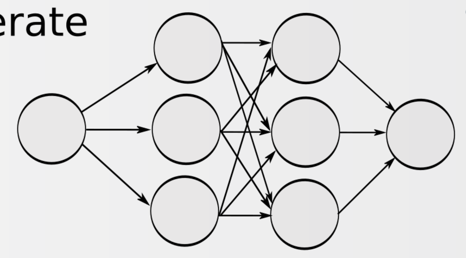
saves both results from the measurement on the clones and sends result from one clone to the bank

cloning is performed at such low frequency that errors resulting from this procedure are bellow the banks denial threshold





the attackers can generate their own banknotes

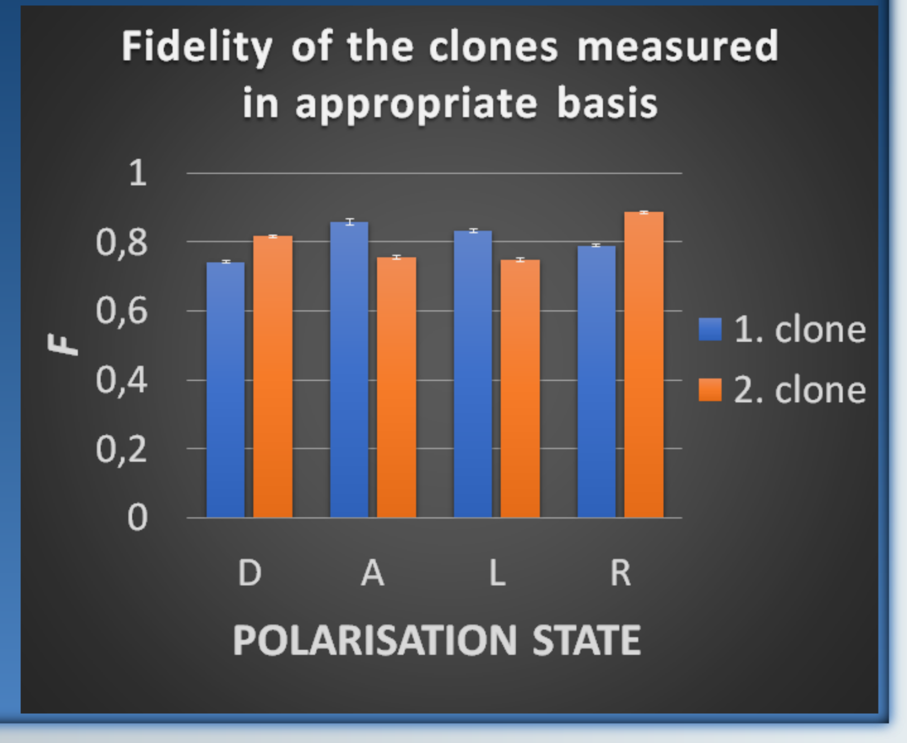


machine learning (or "brute force" method) reveals bank's secret function

Cloning performance

We present a plot of fidelities for both clones F for each measured state.

The average fidelity is always bellow the theoretical threshold value $F \leq 0.856$.



Results

We studied the case when the secret function was a specific hash function known to the attacker.

Hash function:

We generated serial numbers (SN) and encoded the banknotes using 4 hash-based functions (Hash-based Message Authentification Code):
HMAC-MD5
HMAC-SHA512
HMAC-SHA256
HMAC-SHA1.

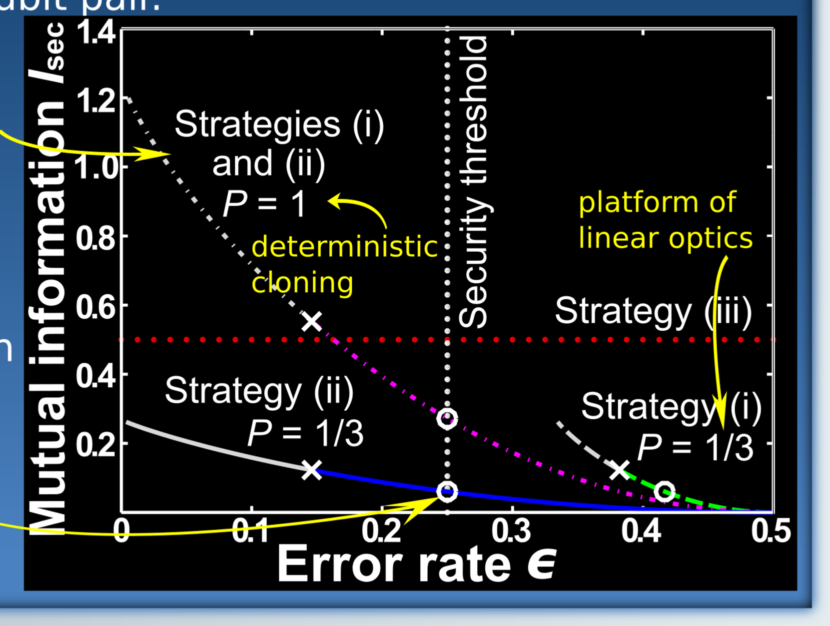
These functions were used for creating hashes from SNs by applying one specific secret number which was subsequently searched by the algorithm. Additional information gained by cloning is then used for guessing the secret number. This is done by calculating the number of agreements (matching qubit pairs) between predictions of the tested encoding and the measurement outcomes on real banknotes (SN).

This plot was evaluated for 4 040 successfully cloned photon pairs (corresponding to 101 SNs used in the experiment). The secret number was searched only among all possible three-digit numbers.

Mutual information

Strategies of the attack can be compared w.r.t. mutual information. This quantity expresses how many bits of information can the attacker obtain upon cloning one qubit pair.

We denote the probability of successful cloning P and error rate ϵ is the probability of an error being reported to the bank.



Affiliation

RCPTM, Joint Laboratory of Optics of Palacky University Olomouc and institute of Physics of Academy of Science of the Czech Republic, 17. listopadu 12, 771 46, Olomouc, Czech Republic

References

[Aaronson2012] S. Aaronson, and P. Christiano, arXiv, 1203.4740 (2012).

[Bozzio2018] M. Bozzio, *et al.* njp Quantum Inf. **4**, 5 (2018).

[Fiurasek2003] J. Fiurasek, PhysRev A **67**, 052314 (2003).

[Wiesner1983] S. Wiesner, ACM SIGACT News **15**, 78-88 (1983).

[Jirakova2018] K. Jirakova, *et al.*, arXiv, 1811.10718 (2018).

This research is supported by the Czech Science Foundation under the project No. 17-10003S and by an internal grant of Palacký University in Olomouc IGA_PrF_2019_008.