Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Information Technology
FH Zentralschweiz

Advanced Topics - Exercise

Prof. Dr. Josef F. Bürgler

I.BA_MOVK, Semesterweek 14

Please write down to solution of the exercises in a consise but comprehensible way. If the computations get too complicated to do it by a hand calculator use python. The solution should be a python worksheet. Numerical results should be accurate to 4 digits. Sketches should be correct qualitatively. At least 75% of the exercises have to be solve satisfactorily. Due time is one week after we have discussed the corresponding topic in class.

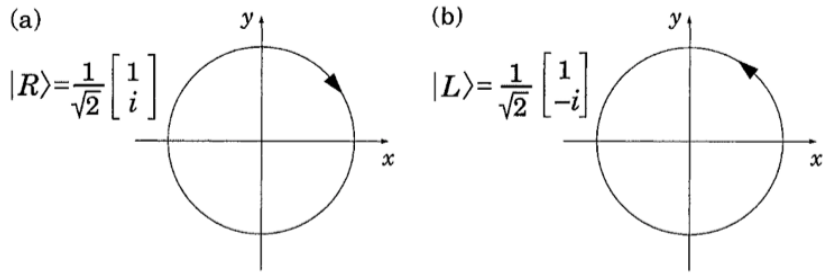
1 Right- and left-hand circularly polarized light

Depicted in the figure are (a) right-hand and (b) left-hand circularly polarized light. The vectors

$$|R\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ i\end{bmatrix},$$
$$|L\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ -i\end{bmatrix}$$

where i is the imaginary unit ($i^2 = -1$) just form a new basis for the state of a photon. Show that the linear polarization emerge as a superposition of the former basis vectors, i.e. show

$$|\leftrightarrow\rangle = \begin{bmatrix}1\\ 0\end{bmatrix} = \frac{1}{\sqrt{2}}\left(|L\rangle + |R\rangle\right),$$
$$|\updownarrow\rangle = \begin{bmatrix}0\\ 1\end{bmatrix} = \frac{i}{\sqrt{2}}\left(|L\rangle - |R\rangle\right)$$



2 BB84

Suppose Alice uses the following polarization states and bit values and Bob measures in the depicted basis. Compute the raw key (bevor reconciliation/error correction and privacy amplification).

Alice's polar. states	$\lvert\nearrow\rangle$	$\lvert\updownarrow\rangle$	$\lvert\updownarrow\rangle$	$\lvert\leftrightarrow\rangle$	$\lvert\searrow\rangle$	$\lvert\searrow\rangle$	$\lvert\updownarrow\rangle$	$\lvert\nearrow\rangle$	$\lvert\leftrightarrow\rangle$
Alice's bit value	1	0	0	1	0	0	0	1	1
Bob's basis	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$

3 Again BB84

In the BB84 protocol

1. what is the probability, that Bob chooses the same basis as Alice?
2. what is the probability, that Eve guesses the correct basis and resends the qubit in the correct state to Bob? Will her interaction be observed in this case?
3. What percentage of bits of the raw key has Bob to discard typically? Note: the shorter key is called **shifted key.**

4 How to find the period of an injective function f

The idea in classical computing would be to choose random x and x' and check, whether $f(x) = f(x')$. If that is the case, then $x' = x + kp$ for some $k \in \mathbb{Z}$. Hence we could find a multiple (kp) of the period p.
It can be shown, that a first guess of p can be made using brute force, by finding a collision in f using approximately $\sqrt{r}$ inputs. Explain!

5 Shor's algorithm to factor 35

Use Shor's algorithm to factor $n = 35$. Start with $m = 11$, and then $m = 2$, $m = 3$. For step 2 use a *classical computer*, i.e. do it by hand!

Have fun with crypto!