
Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar
Hálózati Rendszerek és Szolgáltatások Tanszék

# Polarizációkontroll kvantumkommunikációs rendszerekben

**TDK dolgozat**

Készítette:

Ramadan Erik

Konzulens:

Dr. Kis Zsolt
Wigner Fizikai Kutatóközpont

Dr. Schranz Ágoston
BME-HIT

2023

# Tartalomjegyzék

# 1. fejezet

# Bevezetés

A biztonságos és titkosított kommunikáció napjainkban elengedhetetlenné vált, mivel az életünk számos fontos területén megjelenik, mint például a bankszektorbeli tranzakcióknál, az egészségügyi adatok védelménél és szinte bármilyen internetes üzenetváltásnál. Az eddig nagyon elterjedt és sok téren használt nyilvános kulcsú vagy aszimmetrikus kulcsú titkosítások klasszikus számítógépekkel nehezen megoldható problémákon alapulnak, melyek kvantumszámítógépekkel lehet, hogy könnyen megoldhatóak lesznek. Az egyik ilyen nehéz probléma, egy $N$ egész számnak a prímtényezőkre való felbontása, kvantumosan (a Shor algoritmussal [9]) bizonyítottan $\log(N)$-ben polinomiális időben megoldható lesz, így azok a titkosítások, melyek ezen alapultak gyorsan feltörhetővé válnak. Az egyik legelterjedtebb ilyen nyíltkulcsú titkosítási algoritmusnál, az RSA-nál (Rivest–Shamir–Adleman [8]), leggyakrabban 2048 bites kulcsot használnak, melynek növelése sajnos nem oldaná meg a problémát, mert a feltörés sebessége a kulcshossz logaritmusával arányos.
A kvantumos kulcsmegosztás megoldhatja ezt a problémát, mert szimmetrikus kulcsú titkosítást tesz lehetővé, mely csak próbálgatással törhető fel [4]. A kvantumos kulcsmegosztó rendszerek jelentős része foton alapú, így szükség van egyfoton detektorok használatára, melyek során a detektálás hatásfoka függhet a fény polarizációjától, ezért ennek aktív kontrollja indokoltá válik.
A BME Hálózati Rendszerek és Szolgáltatások Tanszékén egy összefonódott fotonpár alapú kvantumos kulcsmegosztó rendszer fejlesztése van folyamatban, melyben egy szupravezető nanohuzalos egyfoton-detektor (SNSPD, Superconducting Nanowire Single Photon Detector) detektálja a vevőegységben a beérkező fotonokat. A rendszerben használt optikai szálakban a fény polarizációs állapota változik a terjedés során. A feladatom az volt, hogy a fotonokat a polarizáció szerinti szétválasztás után, mikor már nem hordoz információt a polariziációs állapotuk, úgy kontrolláljam egy erre alkalmas eszközzel (MPC320 - Motorized Fiber Polarization Controller), hogy az SNSPD detektor minél hatékonyabban tudja detektálni őket. A detektálás

hatásfokának javulása egyben növeli az egy másodperc alatt szétoszthtató kulcsbitek számát, ami a titkosítható adatmennyiséget szabja meg.

# 2. fejezet

# Elméleti összefoglaló

A következőkben összefoglaltam a kutatási téma alapos megértéséhez szükséges elméleti háttértudást, melyek a fény polarizációs tulajdonsága illetve annak matematikai leírásai, a kvantumos kulcsmegosztás általános formája és a polarizált foton kvantumos információhordozóként való felhasználása.

## 2.1. A fény polarizációs állapota

### 2.1.1. Általános leírás

A fény egy transzverzális elektromágneses hullám, melyről már a 17. század óta tudjuk, hogy van polarizációja. 1670-ben Rasmus Bartholinus felfedezte [3], hogy ha egy fénynyaláb egy romboéderes kalcitkristályon halad át, akkor két nyaláb lép ki belőle, ezzel mutatta meg, hogy a fény két összetevőből áll, melyeket ő *ordinárius*-nak (o-ray) és *extraordinárius*-nak (e-ray) nevezett. Mivel a két komponens más szögben tört meg a kristályban, ezért a kristályt kettős törőnek (birefringent) nevezte. Mindkét komponens eleget tesz a Snellius–Descartes-féle fénytörési törvénynek, de más a törésmutatója a közegnek rájuk nézve.
Később Huygens felfedezte, hogy ha egy második kristályt forgatunk a fény útjában, akkor akár az egyik komponens teljesen eltűnhet és a másiknak maximum erőssége lesz. Ha még 90°-kal elfordítjuk, akkor a másik komponens tűnik el és az első maximum erősségű lesz. 45°-os forgatásnál a két nyaláb erőssége azonos lesz. A fényt ezen tulajdonsága miatt polarizáltnak nevezte.
1820-ban Fresnel elmélete a fényről megmagyarázta az interferenciát, a diffrakciót és a polarizáció jelenségét. Erre építve később megalkották a hullámegyenleteket:

$$\begin{aligned} \nabla^2 E_x(\mathbf{r},t) &= \frac{1}{v^2}\frac{\partial^2 E_x(\mathbf{r},t)}{\partial t^2}, \\ \nabla^2 E_y(\mathbf{r},t) &= \frac{1}{v^2}\frac{\partial^2 E_y(\mathbf{r},t)}{\partial t^2}, \end{aligned} \tag{2.1}$$

ahol $E_x(\mathbf{r},t)$ és $E_y(\mathbf{r},t)$ az elektromos térerősség komponensei, $\mathbf{r}$ a pozíció, $t$ az idő, $v$ a hullám sebessége és $\nabla^2$ a Laplace-operátor. $E_x(\mathbf{r},t)$ és $E_y(\mathbf{r},t)$ merőlegesek a haladási irányra.
Az egyenletrendszer megoldása:

$$\begin{aligned} E_x(\mathbf{r},t) &= E_{0x}\cos(\omega t - \mathbf{k}\cdot\mathbf{r} + \delta_x), \\ E_y(\mathbf{r},t) &= E_{0y}\cos(\omega t - \mathbf{k}\cdot\mathbf{r} + \delta_y), \end{aligned} \tag{2.2}$$

melyekben $\mathbf{k} = (2\pi/\lambda)\,\hat{\mathbf{k}}$ a hullámszámvektor, $\hat{\mathbf{k}}$ a hullámszámvektor irányába mutató egységvektor, $\omega = 2\pi f$ a körfrekvencia, $E_{0x}$ és $E_{0y}$ a maximum amplitúdók és $\delta_x$ és $\delta_y$ a komponensek kezdőfázisai. Ha a koordinátarendszer $z$ tengelye párhuzamos a $\hat{\mathbf{k}}$ vektorral, akkor a (2.2) egyszerűbb alakot vesz fel:

$$\begin{aligned} E_x(z,t) &= E_{0x}\cos(\omega t - kz + \delta_x), \\ E_y(z,t) &= E_{0y}\cos(\omega t - kz + \delta_y), \end{aligned} \tag{2.3}$$

melyben $z$ a vevőtől mért távolság. [3]

### 2.1.2. Speciális esetek

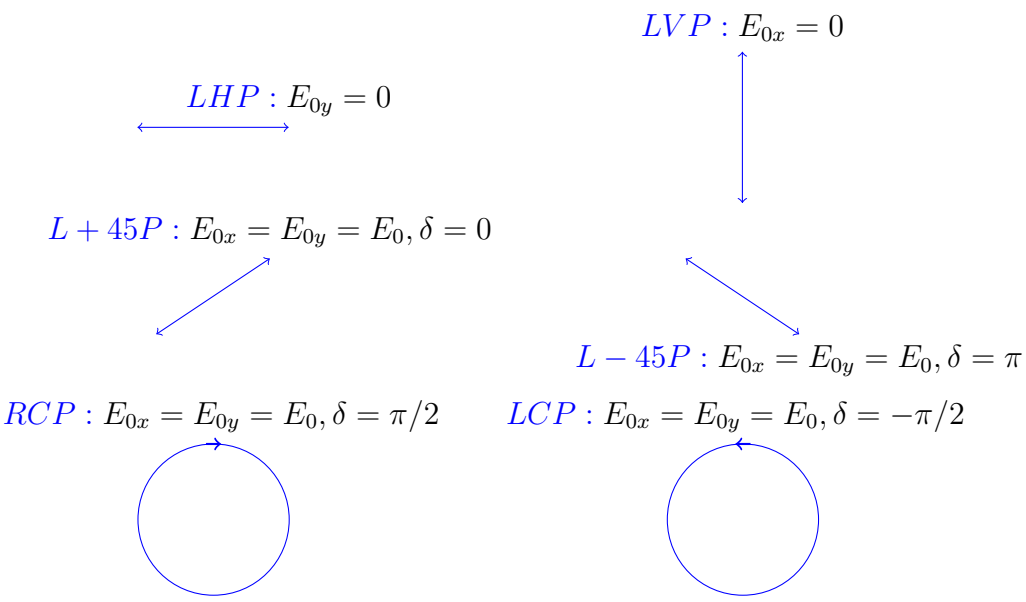
Általános esetben a polarizált fényt szemből (a vevőtől) nézve az elektromos tér vektorának végét követve, annak pályája elliptikus lesz. Amennyiben annak csak $x$ irányú komponense van (azaz $E_{0y} = 0$), akkor horizontális síkban poláros fényt kapunk, vagy az angol nevének rövidítéséből LHP-nek (Linearly Horizontal Polarized light) nevezzük. Egyéb speciális esetek még az LVP (Linearly Vertical Polarized light), L + 45P és L − 45P (Linear ±45° Polarized light) és a cirkulárisan poláros RCP és LCP (Right/Left Circularly Polarized light). Az utóbbi 4 esetben már mindkét komponens jelen van és az L ± 45P kivételével már a fáziskülönbségük ($\delta$) sem nulla [3]. A fény nevezetes polarizációs állapotait szemlélteti a 2.1. ábra.

A polarizált fény leírható egy 2x1-es vektorral, melynek elemei komplexek. Ennek neve Jones-vektor, általános alakja a következő:

$$\begin{bmatrix} E_{0x}e^{i\Phi_x} \\ E_{0y}e^{i\Phi_y} \end{bmatrix}, \tag{2.4}$$

melyben $\Phi_x$ és $\Phi_y$ a kezdőfázisok és $i$ az imaginárius egység. Az elemek abszolútértékének négyzetösszege arányos a fény intenzitásával, de ezt gyakran 1-re normálják.

A fentebb bemutatott 6 speciális esetre is felírhatók a Jones-vektorok, melyeket a 2.1 táblázat foglal össze.




**2.1. ábra.** A fény polarizációs állapotainak szemléltetése.

| Polarizációs állapot | Jones-vektor | *ket* jelölés |
|---|---|---|
| LHP | $\begin{bmatrix}1\\0\end{bmatrix}$ | $\|H\rangle$ |
| LVP | $\begin{bmatrix}0\\1\end{bmatrix}$ | $\|V\rangle$ |
| L+45 | $\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$ | $\|D\rangle = \frac{1}{\sqrt{2}}(\|H\rangle + \|V\rangle)$ |
| L-45 | $\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$ | $\|A\rangle = \frac{1}{\sqrt{2}}(\|H\rangle - \|V\rangle)$ |
| RCP | $\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-i\end{bmatrix}$ | $\|R\rangle = \frac{1}{\sqrt{2}}(\|H\rangle - i\|V\rangle)$ |
| LCP | $\frac{1}{\sqrt{2}}\begin{bmatrix}1\\i\end{bmatrix}$ | $\|L\rangle = \frac{1}{\sqrt{2}}(\|H\rangle + i\|V\rangle)$ |

**2.1. táblázat.** A fény nevezetes polarizációs állapotainak megfelelő Jones-vektorok.

| Optikai eszköz | Jones-mátrix |
|---|---|
| Lineáris polarizátor, mely a **horizontális** fényt engedi át | $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ |
| Lineáris polarizátor, mely a **vertikális** fényt engedi át | $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ |
| Lineáris polarizátor, mely a $\pm$ **45°**-os fényt engedi át | $\frac{1}{2}\begin{bmatrix} 1 & \pm 1 \\ \pm 1 & 1 \end{bmatrix}$ |
| Lineáris polarizátor, mely a $\Theta$ szögű fényt engedi át (a horizontálishoz viszonyítva) | $\begin{bmatrix} \cos^2(\Theta) & \cos(\Theta)\sin(\Theta) \\ \cos(\Theta)\sin(\Theta) & \sin^2(\Theta) \end{bmatrix}$ |
| Jobb cirkuláris polarizátor, mely az **RCP** fényt engedi át | $\frac{1}{2}\begin{bmatrix} 1 & i \\ -i & 1 \end{bmatrix}$ |
| Bal cirkuláris polarizátor, mely az **LCP** fényt engedi át | $\frac{1}{2}\begin{bmatrix} 1 & -i \\ i & 1 \end{bmatrix}$ |

**2.2. táblázat.** Nevezetes polarizációs eszközök Jones-mátrixa.

### 2.1.3. Polarizátorok

Vannak olyan eszközök, melyek csak bizonyos polarizációjú fényt engednek át magukon, azaz egy tetszőleges fényből polarizáltat csinálnak. Ezeket polarizátoroknak hívjuk és egy-egy 2x2-es Jones-mátrixszal tudjuk őket reprezentálni a 2.2 táblázat szerint.

### 2.1.4. Fázistoló eszközök

A kettősen törő kristályok, vagy másnéven fázistolók, között is vannak speciálisak, melyből a gyakorlatban főleg kettőt használnak. Az egyik a $\lambda/2$-es lemez (angol nevén Half-wave plate, vagy HWP), mely úgy van kialakítva, hogy az egyik polarizációs állapotot pontosan egy fél periódussal késleltesse a másikhoz képest. A relatív fáziseltolódást a következőképpen lehet leírni: $\Gamma = \frac{2\pi\Delta n L}{\lambda_0}$, melyben $\Gamma$ a relatív fáziseltolódás, $\Delta n$ a törésmutatók különbsége, $L$ a kristály vastagsága és $\lambda_0$ a fény vákuumbeli hullámhossza.
Jól látszik tehát, hogy ahhoz hogy egy ilyen kristályt megalkossunk, nagyfokú precizitás szükséges és csak egy bizonyos hullámhossztartományon működik elfogadhatóan. Az $L$ vastagság lehet akár olyan is, hogy ne $\pi/2$ legyen a fázistolás, hanem $\pi/2 + k \cdot 2\pi$, ahol k egy nemnegatív egész szám.
A másik speciális lemez a $\lambda/4$-es lemez (angol nevén Quarter-wave plate, vagy

QWP), mely annyiban különbözik, hogy az egyik polarizációs állapotot egy negyed periódussal késlelteti a másikhoz képest.
A HWP egy lineárisan polarizált fény polarizációjának síkját tudja megváltoztatni veszteség nélkül, míg a QWP a fény cirkularitását tudja megváltoztatni, tehát egy lineárisan polarizált fényből tud elliptikusan polarizáltat csinálni vagy fordítva. Ezeknek a lemezeknek szokás a gyors tengelyét (fast axis) meghatározni úgy, hogy azt tekintjük gyors tengelynek, amelyre párhuzamos polarizációjú fény a leggyorsabban megy át a kristályon és a kristály forgatásakor ennek a tengelynek a pozícióját mondjuk meg. Ezeknek a speciális fázistoló lemezeknek a Jones-mártixait láthatjuk a 2.3. táblázatban.

| Fázistoló | Jones-mátrix |
|---|---|
| QWP, melynek gyors tengelye vertikális | $e^{\frac{i\pi}{4}} \begin{bmatrix} 1 & 0 \\ 0 & -i \end{bmatrix}$ |
| QWP, melynek gyors tengelye horizontális | $e^{-\frac{i\pi}{4}} \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$ |
| QWP, melynek gyors tengelye $\phi$ szögben van elfordítva a horizontálishoz képest | $e^{-\frac{i\pi}{4}} \begin{bmatrix} \cos^2\phi + i\sin^2\phi & (1-i)\sin\phi\cos\phi \\ (1-i)\sin\phi\cos\phi & sin^2\phi + i\cos^2\phi \end{bmatrix}$ |
| HWP elfordítva $\phi$ szöggel | $\begin{bmatrix} \cos(2\phi) & \sin(2\phi) \\ \sin(2\phi) & -\cos(2\phi) \end{bmatrix}$ |
| HWP, melynek gyors tengelye $\phi$ szögben van elfordítva a horizontálishoz képest | $e^{-\frac{i\pi}{2}} \begin{bmatrix} \cos^2\phi - \sin^2\phi & 2\cos\phi\sin\phi \\ 2\cos\phi\sin\phi & \sin^2\phi - \cos^2\phi \end{bmatrix}$ |

**2.3. táblázat.** Fél- és negyedhullámú lemezek Jones-mátrixai.

Egy általános fázistoló lemeznek is felírható a Jones-mátrixa, melyben szereplő $\eta$ a relatív fázistolás a gyors és a lassú tengely között.

Általános fázistoló: $$e^{-\frac{i\eta}{2}} \begin{bmatrix} \cos^2\phi + e^{i\eta}\sin^2\phi & (1-e^{i\eta})\cos\phi\sin\phi \\ (1-e^{i\eta})\cos\phi\sin\phi & \sin^2\phi + e^{i\eta}\cos^2\phi \end{bmatrix}$$

A Jones-kalkulust használva egy tetszőleges polarizációjú bemeneti fény vektorának transzformációját kapjuk meg, melyet azok az eszközök váltanak ki, melyeken a fény áthalad.

### 2.1.5. Stokes-paraméterek

A fény polarizációjának grafikus ábrázolására Poincaré javasolt egy módszert, melyben a Descartes-féle koordinátarendszerben egy gömbön ábrázoljuk azt. Ehhez szükségünk van a Stokes-paraméterekre, melyek a következők:

- $S_0$: A fény teljesítménye.
- $S_1$: A fény $LHP$ és $LVP$ komponensének különbsége.
- $S_2$: A fény $L+45P$ és $L-45P$ komponensének különbsége.
- $S_3$: A fény $RCP$ és $LCP$ komponensének különbsége.

Ezeket kissé módosítva, $S_0$-al lenormálva kapunk 3 paramétert $(S_1, S_2, S_3)$, melyet a koordinátarendszer x, y és z tengelyén ábrázolunk. Az így kapott paraméterek egyenletei:

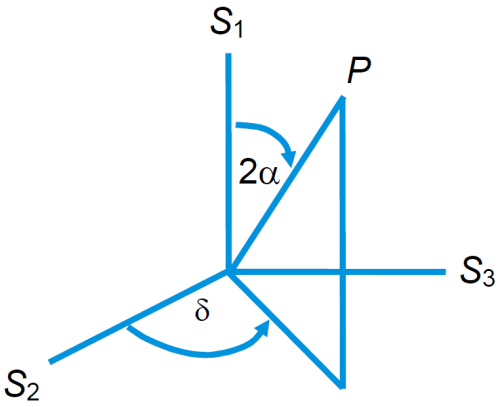
- $S_0 = E_{0x}^2 + E_{0y}^2 \to 1$,
- $S_1 = E_{0x}^2 - E_{0y}^2 \to \cos(2\alpha)$,
- $S_2 = 2E_{0x}E_{0y}\cos\delta \to \sin(2\alpha)\cos\delta$,
- $S_3 = 2E_{0x}E_{0y}\sin\delta \to \sin(2\alpha)\sin\delta$, $\delta = \delta_y - \delta_x$.

$2\alpha$ és $\delta$ a gömbi koordinátarendszer szögei, melyek kifejezhetők a Stokes-paraméterekből:

$$\begin{aligned} 2\alpha &= \cos^{-1}\left(\frac{S_1}{S_0}\right), \quad 0 \leq 2\alpha < \pi, \\ \delta &= \tan^{-1}\left(\frac{S_3}{S_2}\right), \quad 0 \leq \delta < 2\pi. \end{aligned} \tag{2.5}$$

A paramétereket összefoglalja a 2.2-es ábra.

Fontos megjegyezni, hogy csak a teljesen polarizált fényre igaz az ${S_1}^2 + {S_2}^2 + {S_3}^2 = 1$ összefüggés, tehát az ezeket reprezentáló pontok egy gömb (Poincaré-gömb) felszínén helyezkednek el, míg egy általános, részben polarizált fény egy olyan ponttal jellemezhető, mely a gömb belsejében van.
Mindhárom tengely a [-1,1] intervallumban értelmezett és a tengelyek végpontjain a már bemutatott speciális polarizációs állapotok (LHP, LVP, L+45°, L-45°, RCP és LCP) helyezkednek el, amit a Stokes-paraméterek jellemzéséből is látható (pl.: $S_1$: az LHP és LVP komponensek különbsége. Két szélső esete 1 és -1, melyek megfelelnek LHP-nak és LVP-nek).
A Stokes-paraméterek lehetővé teszik az ábrázolást, de a Jones-vektorokkal és mátrixokkal könnyebben lehet számolni. A két rendszer között az áttérés a következő:




**2.2. ábra.** Stokes-paraméterek és a gömbi koordinátarendszer szögei [3]

Vegyünk egy általános Jones-vektort, melynek elemei $X$ és $Y$ komplex számok. A Stokes-paramétereket az

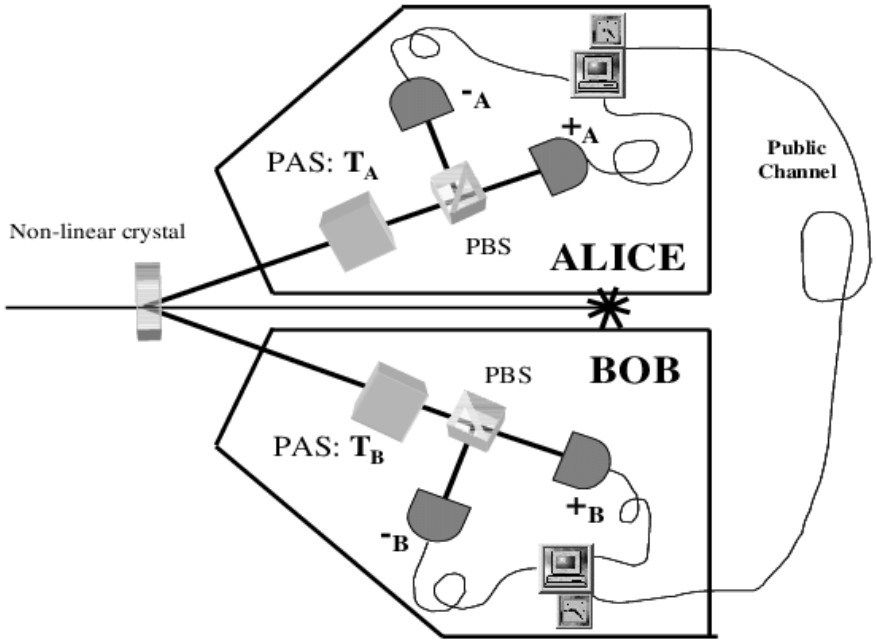
$$\begin{aligned} S_0 &= |X|^2 + |Y|^2 \\ S_1 &= |X|^2 - |Y|^2 \\ S_2 &= 2 \cdot \Re(X \cdot \bar{Y}) \\ S_3 &= 2 \cdot \Im(X \cdot \bar{Y}) \end{aligned} \tag{2.6}$$

egyenletekkel tudjuk kiszámolni, ahol $\Re$ a valósrészt és $\Im$ a képzetes részt jelenti, míg $\bar{Y}$ az $Y$ komponens komplex konjugáltját jelöli [7].

## 2.2. Kvantumos kulcsmegosztás

A kvantumos kulcsmegosztás (QKD - Quantum Key Distribution) lehetővé teszi a titkos kulcsok biztonságos megosztását. Ez a módszer nem a matematikailag nehezen kiszámítható és nehezen megoldható komplex problémákon alapul, hanem fizikai törvényeken. Ilyen fizikai törvény a *No-cloning theorem* vagy nemklónozhatósági tétel, mely azt mondja ki, hogy nem lehet egy tökéletes másolatot csinálni egy tetszőleges ismeretlen kvantumállapotról. Ennek a tételnek az értelmében nem lehet egy kvantumkommunikációs csatornát úgy lehallgatni, hogy abban ne okozzunk olyan változást, amelyet a kulcsszétosztásban résztvevő felek ne tudnának észlelni [4].
A tanszéken épülő ún. *diszkrét változójú* QKD-rendszer a kvantumösszefonódást használja ki, mégpedig úgy, hogy egy polarizációsan összefonódott fotonpár egyik tagját elküldjük az egyik félnek (Alice), míg a másikat a másik félnek (Bob) és ők mindketten megmérik a foton polarizációját két bázis közül az egyikben, majd ezután a bázisokat egyeztetik klasszikus csatornán. Ez az Eckert-féle kvantumos kulcsmegosztó protokoll, röviden E91 [6]. Azokat az eseteket, amelyeknél különbö-

ző bázisban mértek, eldobják, a maradék esetekben, ami statisztikailag körülbelül a fotonpárok fele, a kvantumösszefonódás jelensége miatt biztosak lehetnek benne, hogy egymásra ortogonális polarizációs állapotot mértek a két fotonon [1]. A mérések után az állapotokhoz egy bizonyos, előre megbeszélt módon rendelnek biteket és így megkapják a kulcsot, lásd 2.3. ábra [4].




**2.3. ábra.** QKD összefonódott fotonpárral [2]

## 2.3. Polarizáció mint kvantumbit

A kvantumbit, vagy másnéven qubit a kvantuminformatika alapegysége, mely megfeleltethető a klasszikus informatikában használt bitnek, azzal a lényeges különbséggel, hogy míg egy klasszikus bit két állapot egyikét tudja felvenni (0 vagy 1), egy qubit e két állapot szuperpozíciójában tud létezni mindaddig, amíg meg nem mérjük azt. Egy általános kvantumállapotot egy bizonyos *ket*-es jelöléssel írhatjuk fel [2.7], melyben $|\psi\rangle$ (ejtsd: *ket pszí*) a leírni kívánt állapot, melyet a $|0\rangle$, $|1\rangle$ bázisban adunk meg, $\alpha$ és $\beta$ komplex valószínűségi amplitúdókkal súlyozva, melyek abszolútértékeinek négyzetösszege 1-et kell adjon eredményül [2.8]. Ezek az abszolútérték-négyzetek megadják, hogy mekkora valószínűséggel mérünk majd $|0\rangle$ illetve $|1\rangle$ állapotot [5]:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2.7}$$

$$|\alpha|^2 + |\beta|^2 = 1\,. \tag{2.8}$$

A 2.1-es táblázatban láthatjuk, hogy ha a két bázisvektort a horizontális és vertikális polarizációs állapotnak választjuk meg, akkor a poláros fényekre alkalmazhatóak ugyanezek a *ket*-es jelölések és így megfeleltethető egy foton polarizációja egy qubitnek. A fotonok polarizációjára is igaz, hogy képes szuperpozícióban lenni és amint megmérjük egy bizonyos bázisban, a szuperpozíció összeomlik és beáll a két bázis közül az egyikbe, az $|\alpha|^2$ és $|\beta|^2$ valószínűségek szerint.
Az előzőekre egy példa az L+45 polarizációs állapot, mely felírható a $|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ egyenlettel. Megállapítható, hogy itt $\alpha$ és $\beta$ is egyaránt $\frac{1}{\sqrt{2}}$-vel egyezik meg, melynek az abszolútérték-négyzete $\frac{1}{2}$, azaz egy ilyen állapotú fotont megmérve a horizontális-vertikális bázisban, mindkét bázisállapotot azonos (50%) valószínűséggel kapjuk.

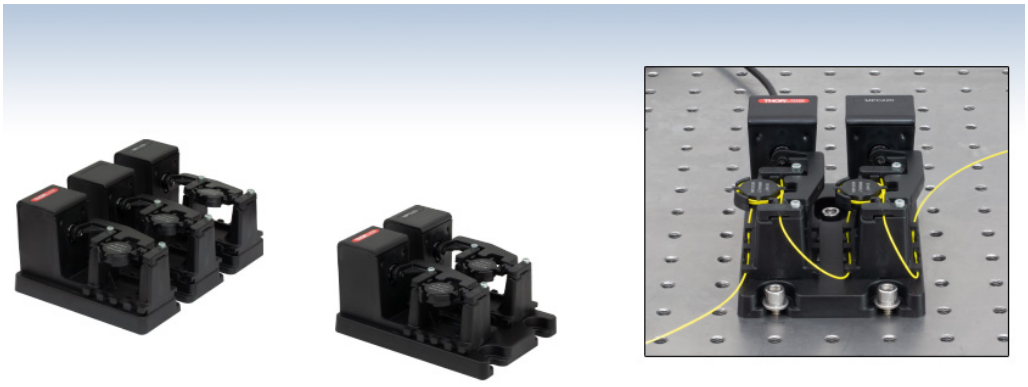
# 3. fejezet

# Szimuláció

A munkám során írtam egy programot Python nyelven, melyben különböző mértékben hibás $\lambda/2$-es és $\lambda/4$-es lemezek hatását tudom szimulálni különböző polarizációjú bemeneti fényekre. A program legfőbb célja az volt, hogy jobban megismerjem ezen lemezek elméleti működését és azt, hogy ezeket forgatva egy bizonyos bemeneti fényből a Poincaré-gömb hány százalékát tudjuk lefedni.

## 3.1. Polarizációkontroller

Az eszköz, amelyet szimuláltam, az MPC320 „Motorized Fiber Polarization Controller", mely három, külön motorral forgatható tárcsából áll. A tárcsákra fel van tekerve az optikai szál, ezáltal megfeleltethetők a korábban bemutatott fázistoló lemezeknek (a két szélső egy-egy $\lambda/4$-es lemeznek, míg a középső egy $\lambda/2$-es lemeznek). A motorral a tárcsákat elforgatva megváltoztathatjuk a szálon áthaladó fény polarizációs állapotát.



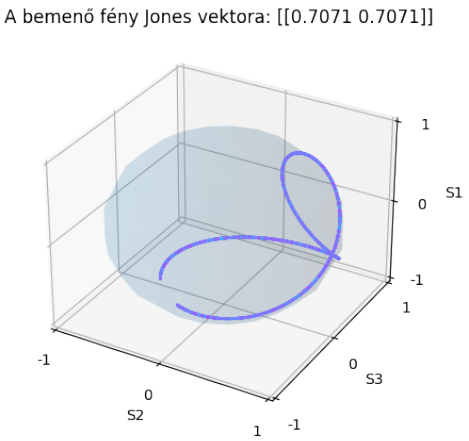
**3.1. ábra.** MPC320 polarizációkontroller [13]

A tárcsák egyesével forgathatók 0 és 170° között, 0.12°-os felbontással. A maxi-

mum forgatási sebesség 400°/mp és az eszköz számítógéphez csatlakoztatható Micro USB Type B kábellel. A polarizációkontrollernek van egy, a Thorlabs honlapjáról letölthető, vezérlőszoftvere, mely rendelkezik grafikus kezelőfelülettel, de lehet programkóddal is irányítani.

## 3.2. Lemezek szimulálása

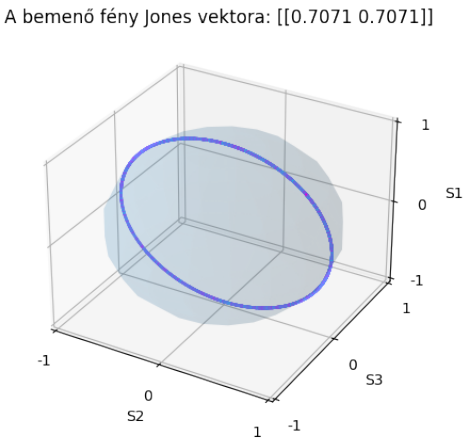
Első lépésként három fázistoló lemez hatását szimuláltam külön-külön (3.2. és 3.3. ábra) és egyszerre is, mert az előbbiekben bevezetett eszköz is ennyit tartalmaz. A fázistoló lemezekhez a fent említett Jones-mátrixos leírást alkalmaztam és a betáplált fényt is felírtam a Jones-vektoros formájában, mely lehetett LHP, LVP, L+45P, L-45P, RCP, LCP vagy akár egy általánosabb polarizált fény, majd ezeket a megfelelő sorrendben összeszoroztam és a kapott fénynek az előzőekben említett módon kiszámítottam a Stokes-paramétereit, melyet ábrázoltam egy Poincaré-gömbön.




**3.2. ábra.** QWP forgatásának hatása L+45P fényre

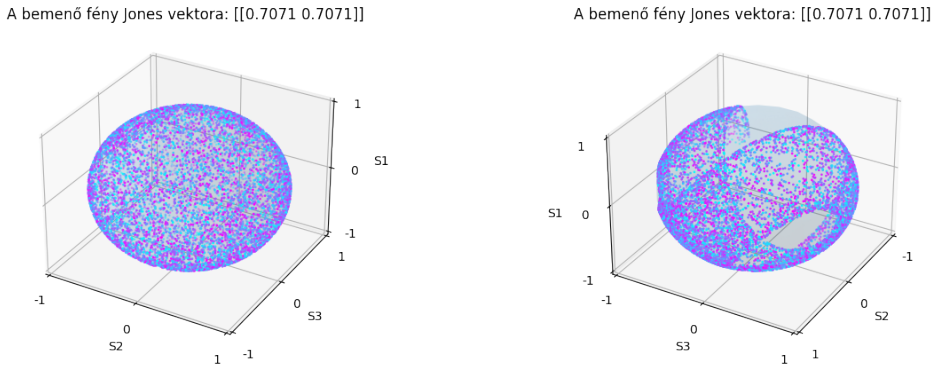
## 3.3. Ábrázolás

A program sorsol több ezer random, 0 és 170 közötti számhármast, melyek a három lemez fokban mért pozícióját jelzi. Ezt a szöget a Jones-mátrix képlete alapján a horizontális tengelyhez kell viszonyítani. Az így kapott beállítások mindegyikére kiszámolja a kimenő fény Stokes-paramétereit (ezekre a továbbiakban „generált pontok”-ként hivatkozom), majd ezeket ábrázolja, így kapunk egy képet arról, hogy mekkora részét tudjuk lefedni az előbb említett gömbnek. A random számhármasok számának növelésével egyre jobban megközelítjük a tényleges lefedhető felszín




**3.3. ábra.** HWP forgatásának hatása L+45P fényre

ábráját, de ez a számítási feladatok számát, így a program futásának idejét is, jelentősen megnövelheti.



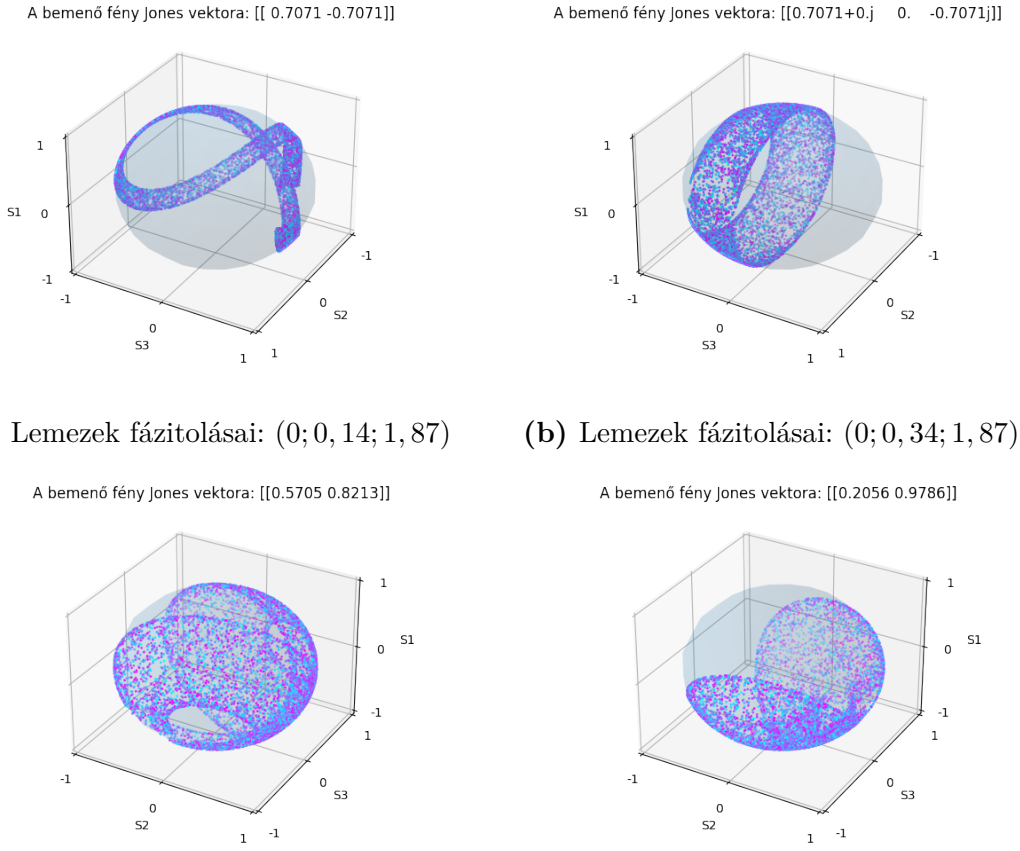

**(a)** Kicsit hibás lemezek **(b)** Nagyon hibás lemezek

**3.4. ábra.** A Poincaré-gömb lefedése fix kiindulóállapotból a fázistoló lemezek forgatása által.

A 3.4. ábrán a lefedettség látható két speciális esetben: a baloldalin a három lemez csak kicsit működik hibásan (a lemezek fázistolása radiánban kifejezve $(1,17; 3,64; 1,97)$ az ideális $(1,57; 3,14; 1,57)$-hez képest), míg a jobboldalin az egyik lemez szinte egyáltalán nem forgat fázist és egy másik lemez csak egy kicsit (a lemezek fázistolása radiánban kifejezve $(0,57; 0; 1,97)$. A második esetben a gömb körülbelül 78%-a van csak lefedve, míg az elsőben a lefedettség szinte 100%-os a tesztelés alapján.

A szimulációból az látszik, hogy nagy a hibatűrő képessége ennek a rendszernek és amennyiben mind a három lemez működik, nem feltétlenül kell, hogy tökéletesek

legyenek ahhoz, hogy a lefedettség közel 100%-os legyen tetszőleges bemenő fénnyel való vizsgálatnál. Amennyiben viszont egy lemez egyáltalán nem forgat fázist, akkor előfordulhat, hogy a gömb bizonyos részein lévő pontok által reprezentált polarizációs állapotokat nem vagyunk képesek előállítani az adott bemenő fényből. A 3.5. ábrán ilyen extrém esetekre láthatunk pár példát.



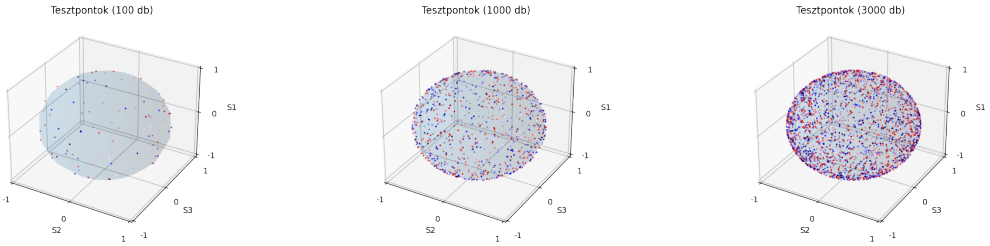

**(a)** Lemezek fázitolásai: $(0; 0,14; 1,87)$ **(b)** Lemezek fázitolásai: $(0; 0,34; 1,87)$

**(c)** Lemezek fázitolásai: $(0,57; 0; 2,07)$ **(d)** Lemezek fázitolásai: $(0,97; 1,04; 0)$

**3.5. ábra.** Extrém esetek, melyekben az egyik lemez egyáltalán nem forgat fázist.

## 3.4. Teszpontok

A gömb lefedettségének vizsgálatához a program random tesztpontokat generál egyenletes eloszlással a gömb felszínén. A tesztelés pontosságát javíthatja a tesztpontok számának növelése, mivel így azok jobban lefedik a gömb felszínét (3.6. ábra), de túl sok tesztpont használata feleslegesen hosszúvá teszi a program futásidejét.




**(a)** 100 db **(b)** 1000 db **(c)** 3000 db

**3.6. ábra.** A Poincaré-gömb lefedettségének változása a tesztpontok számának növelése függvényében.

A lefedettséget az algoritmus százalékban határozza meg, úgy, hogy az összes teszponton végigiterálva megnézi, hogy van-e a egy bizonyos környezetében még nem megtalált generált pont és ha van, akkor azt a generált pontot megtaláltnak tekinti. A ciklus végén a megtalált generált pontok számát elosztja a tesztpontok számával, így kapunk egy 1-nél kisebb értéket, melyet százalékosan ábrázolunk.

A tesztpontok generálásánál fontos szempont volt, hogy bár random generáljuk, a gömb felszínén egyenletes eloszlásúak legyenek, mivel így tudjuk biztosítani a lefedettség vizsgálatának hitelességét. Ezt a program úgy éri el, hogy generál páronként sok random, 0 és 1 közötti értéket egyenletes eloszlással, majd ezekből kiszámolja $\theta$-t és $\phi$-t és azokat átszámolva megkapjuk a tesztpontok koordinátáit.

$$\begin{aligned} \theta &= \arccos(2 \cdot \text{rand} - 1) \\ \phi &= 2 \cdot \pi \cdot \text{rand} \\ X &= \sin(\theta) \cdot \cos(\phi) \\ Y &= \sin(\theta) \cdot \sin(\phi) \\ Z &= \cos(\theta) \end{aligned} \tag{3.1}$$

Itt rand az egyenletesen generált random számot jelöli, míg X, Y és Z a Descartes-féle derékszögű koordinátarendszerben vett értékek.

# 4. fejezet

# Tesztelés és mérés

A polarizációkontroller modellezésésvel megismerhettük, hogy hogyan működne egy ideális eszköz és azt is megvizsgáltuk, hogy mennyire okozhat problémát az, ha nem teljesen tökéletesen működik. Mindezek után leteszteltük az eszköz működését és lemértük a kvantumos kulcsmegosztó rendszerbe való beiktatásának hatását.

## 4.1. Polariméterrel való tesztelés

A valódi rendszeren történő mérés előtt a polarizációkontroller hatását megvizsgáltam egy olyan összeállításban, melyben annak polarizációforgató hatása közvetlenül vizsgálható. A forrás ebben az esetben egy lézerdióda volt, melyből kijövő optikai szál fel volt tekerve a polarizációkontrollerre, és azon áthaladva a benne haladó fényt becsatoltuk egy polarizációmérésre alkalmas eszközbe, mely ebben a rendszerben vevőegységként funkcionált.

### 4.1.1. Polariméter

A tanszék laborjában megismerkedhettem egy PAX1000IR2(/M) típusú polariméterrel (4.1. ábra), melyet a Thorlabs forgalmaz és gyárt.

#### 4.1.1.1. Általános információk és paraméterek

A polarimétert 900 és 1700 nm közötti hullámhosszú fény analizálására tervezték és $-60$ dBm és 10 dBm közötti érzékenysége van (azaz $10^{-6}$ mW és 10 mW közötti fényt tud érzékelni). A mintavételi frekvenciája 30 minta/s alapbeállításoknál és 400 minta/s a maximálás beállításnál.

A műszer tudja mérni a fény teljesítményét, a polarizáltságának mértékét, a polarizáció ellipticitását, a Stokes-paramétereket, a kioltási arányt (azaz a fény

**4.1. ábra.** PAX1000IR2(/M) polariméter [14]

intenzitásának a legnagyobb és a legkisebb értéke közötti arányt), polarizáció függő veszteségeket és a polarizációs módusdiszperziót [14].
Az eszköz USB 2.0 Mini-B-n keresztül csatlakoztatható számítógéphez, és van egy saját kezelőfelülete, melyet a Thorlabs oldaláról letölthető szoftver által lehet elérni. Az értékeket manuálisan, de akár programmal is ki lehet olvasni.

#### 4.1.1.2. Működési elve

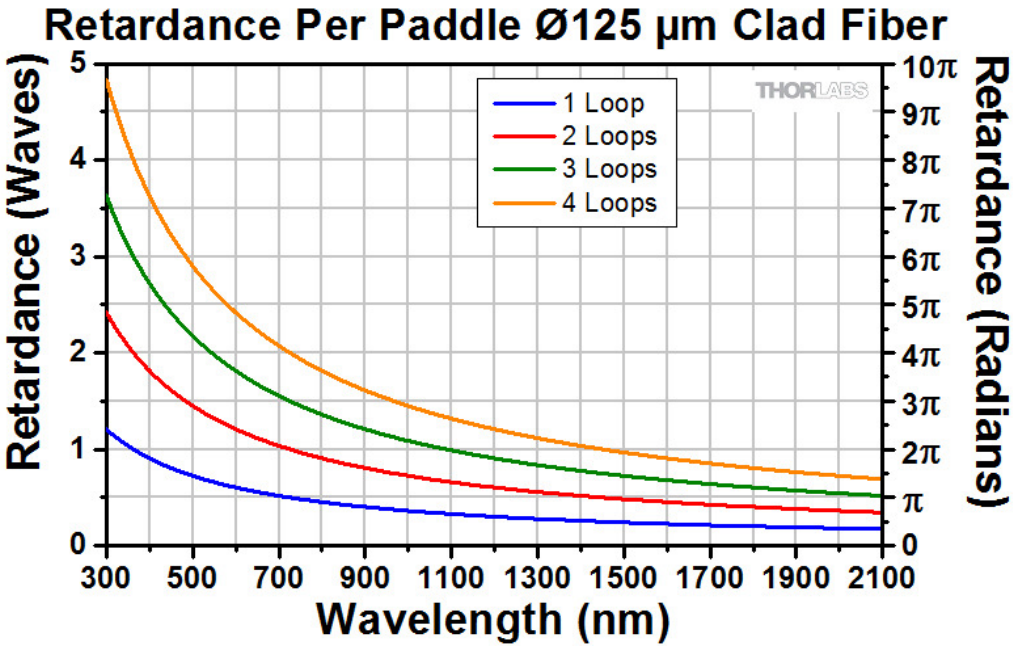
A beérkező fénynek monokromatikusnak és koherensnek kell lennie, és ismernünk kell a hullámhosszát. A polarimétert három részre lehet bontani, egy forgó $\lambda/4$-es lemezre (QWP), egy fix irányítottságú lineáris polarizátorra és egy fotodiódára.
A polarizátor mindig csak egy adott iránnyal párhuzamos polarizációjú fényt engedi át és az előtte forgó $\lambda/4 - es$ lemez folyamatosan változtatja a bejövő fény polarizációját, így a fotodiódára folyamatosan és periodikusan változó intenzitású fény esik, mely ezt a modulált intenzitást méri. Ennek a jelnek a Fourier-analízisával a Stokes-paraméterek meghatározhatók.
A PAX1000 egy úgynevezett „True Zero Order" QWP-t használ, ami azt jelenti, hogy úgy alakították ki, hogy a hullámhosszfüggő változásokat minimalizálták, tehát minimális kromatikus diszperzióval rendelkezik, és ezért nagyobb hullámhossztartományon használható.

### 4.1.2. Csatlakozás az eszközökhöz

A két előzőekben tárgyalt eszközhöz írtam egy programkódot, mely egyszerre csatlakozik rájuk és a polarizációkontrollert képes vezérelni, míg a polariméterből képes kiolvasni a mért adatokat. A csatlakozást a Thorlabs hivatalos oldalán talált segédletek alapján valósítottam meg, ami után az eszközök vezérlése egyszerű parancsokkal lehetséges.

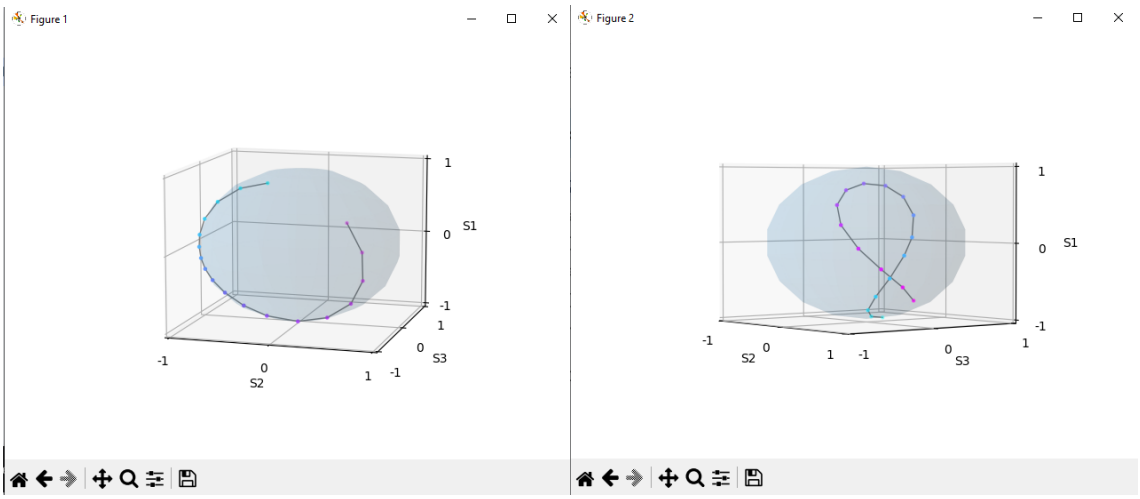
### 4.1.3. Polarizációkontroller tesztelése

A polarizációkontroller három tárcsáját úgy állítottuk be, hogy a Thorlabs útmutatója szerint az első és a harmadik egy $\lambda/4$-es, míg a második egy $\lambda/2$-es lemezként viselkedjen. Ezt a tárcsákra tekert optikai szál meneteinek számával lehet beállítani. A 4.2 diagramról leolvasható, hogy az általunk használt 1550 nm hullámhosszú fénynél a 125 µm keresztmetszetű optikai szálat kétszer kell a tárcsa köré tekerni, hogy az $\pi$ radiánnal késleltesse a fénynek az egyik polarizációjú komponensét a rá merőleges polarizációjú komponenséhez képest. Így kaphatunk $\lambda/2$-es lemezt, míg egyszeres körbetekeréssel körülbelül $\pi/2$-es késleltetést kapunk, amely megfelel egy $\lambda/4$-es lemez működési elvének.
A tárcsákat egyesével le is teszteltem, hogy tényleg úgy működnek-e mint egy ideális QWP vagy HWP (4.3. ábra).




**4.2. ábra.** Késleltetési paraméterek [13]

A tesztelés során megállapítottuk, hogy a tárcsák nem működnek az elvártnak megfelelően, mivel azokat végigforgatva nem az elvárt, ideális lemezekkel megegyező, változást mértük a polarizációs állapotokban. A mérések során a tárcsák hiszterézises jelenséget is mutattak, tehát egy állapoton áthaladva, majd abba visszatérve nem teljesen ugyanazt a polarizációs állapotot kaptuk, ami még jobban megnehezíti az optimumkeresést.




**(a)** $\lambda/4$-esként beállított **(b)** $\lambda/2$-esként beállított

**4.3. ábra.** Fázistoló tárcsák tesztelése

### 4.1.4. Optimumkereső algoritmusok

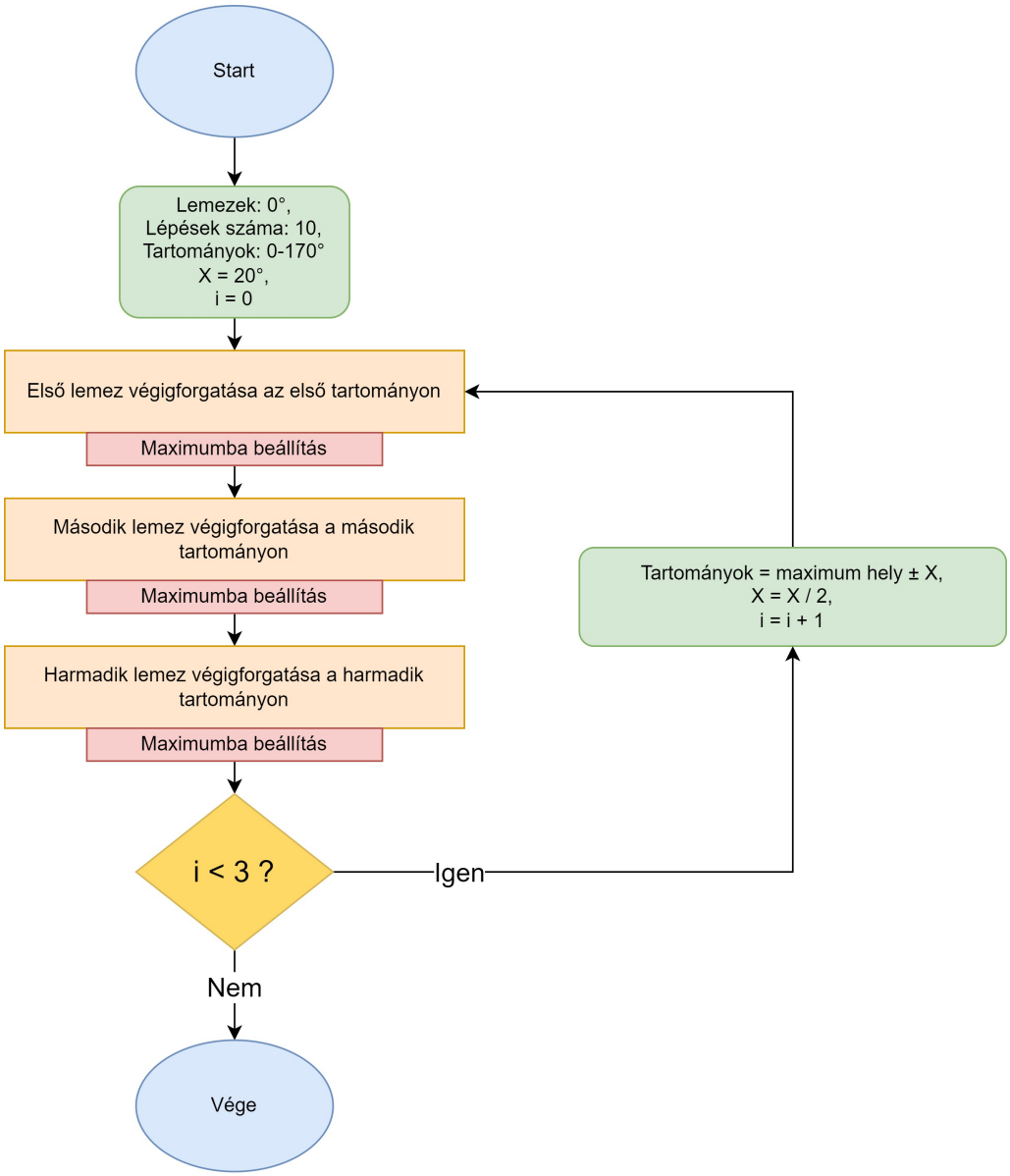
Az optimumkereső algoritmusok feladata az volt, hogy a polarizációkontroller irányításával és a polariméter által mért Stokes-paramétereket használva a fényt az általunk kívánt SOP-be (State of Polarization) állítsák be. Többfajta algoritmus működését teszteltem a rendszeren, majd ezeknek működéseit elemeztem.

#### 4.1.4.1. Végigpásztázás

Az első algoritmus működése és megvalósítása is elég egyszerű. A program beállítja az összes tárcsát 0°-os pozícióba, majd az egyikkel 10°-onként végiglépked a 170°-os szélső állapotig, és egyesével megméri a pontokban mérhető hibajelet, mely a kívánt és a mért SOP különbsége, azaz az általuk reprezentált pontok közötti távolság. A pontokat egy egységsugarú gömbön tudjuk ábrázolni. A ciklus lefutása után beállítja a tárcsát arra az állapotra, ahol a hibajel a legkisebb volt. Ezt megcsinálja a másik két tárcsával is, majd az optimális beállításoktól mindkét irányban megvizsgál egy kisebb tartományt hasonló módon, kisebb lépésközökkel.
Az algoritmus bizonyos állapotokat nagyon nagy pontossággal meg tudott közelíteni, akár 0,01 egység körüli környezetében is az egységsugarú gömbön, míg egyes állapotokat nem tudott, csak 0,3 egységre. Ezt valószínűleg a lokális minimumokba való beragadás okozhatja, melyet ez az algoritmus nem tud kezelni (4.4. ábra).

#### 4.1.4.2. Random pontok vizsgálata

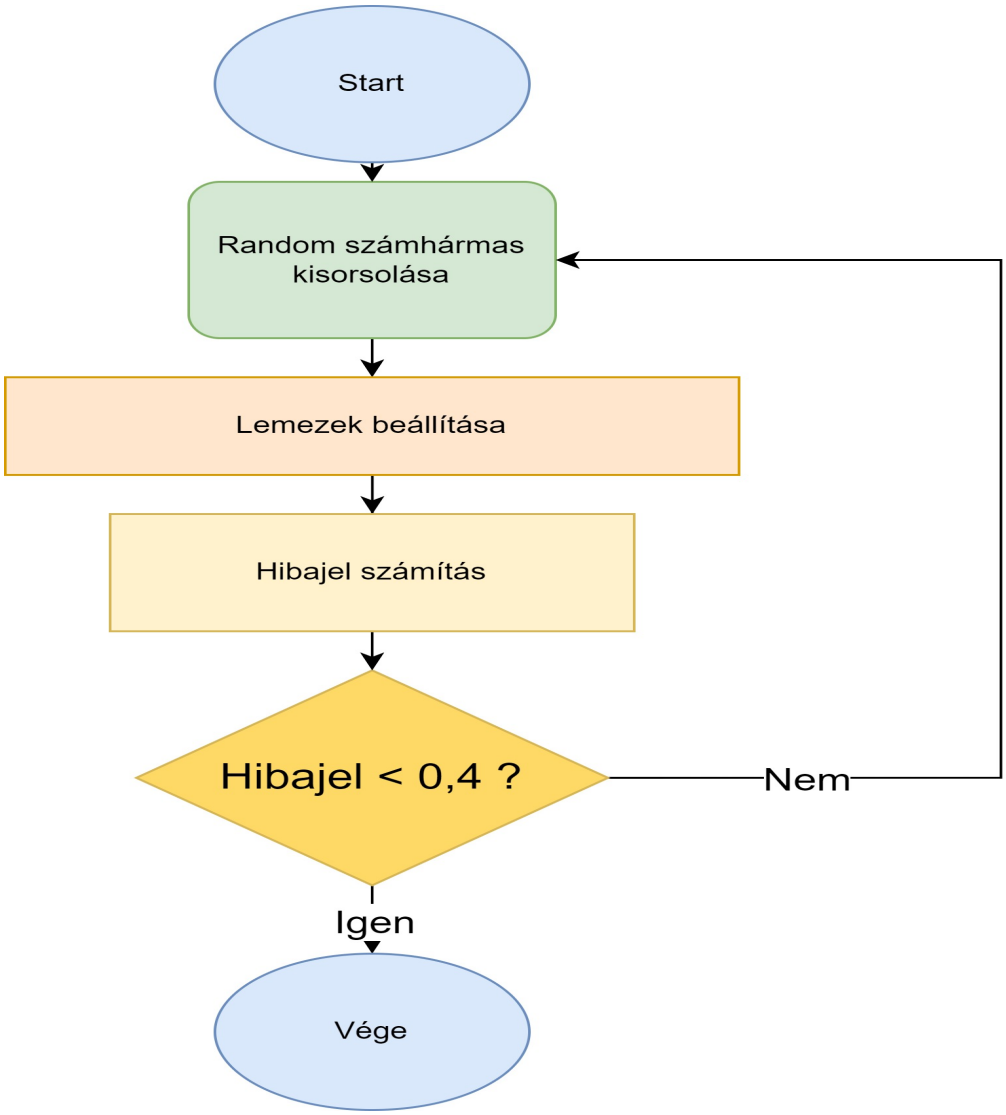
A második, szintén egyszerű algoritmus, melyet implementáltam és teszteltem, 0 és 170° közötti random sorsolt szögekbe állította be a lemezeket, majd megmérte az SOP-t és kiszámolta a hibajelet, az előző algoritmussal megegyező módon. Ezt ad-




**4.4. ábra.** Végigpásztázó algoritmus

dig ismételte, míg nem kapott egy bizonyos határérték alatti hibajelet. Itt nem volt meg a veszélye a lokális minimumokba való beragadásnak, mivel a számhármasok egymástól függetlenül random generálódtak.

Az algoritmus sokszor nagyon hamar megtalálta a kívánt állapot kis sugarú környezetét, viszont volt olyan is, hogy több mint 40 random számhármas kellett egy nem túl szigorú 0,4 hiba alatti pont megtalálásához, tehát ez az algoritmus nem kiszámítható gyorsaságú és elméletben akár több óráig is tarthat. Átlagosan 0,4 hiba alatti pontot keresve, 1-2 percig tartott az algoritmus futása. (4.5. ábra)




**4.5. ábra.** Random pontok vizsgálata

#### 4.1.4.3. Kombinált algoritmus

A harmadik algoritmus az előző kettőnek az előnyeit ötvözi azzal, hogy először néhány random pontot megvizsgálva egy nagyjából jó állapotot keres, majd azt tökéletesíti a pásztázó algoritmussal egy kis tartományon. Ez jóval pontosabb állapotot képes beállítani mint a második algoritmus és ki tudja kerülni a lokális minimumokat a random pontokból való indulásokkal, így az első algoritmusnál is jobb.

#### 4.1.4.4. Kombinált algoritmus irányított találgatással

A kombinált algoritmus, bár pontos volt, és el tudta kerülni a lokális minimumokat, esetenként több mint 7 percig futott, mert sokáig nem talált olyan állapotot, aminél a hiba az előre beállított limit alatt lett volna. Ezt az okozta, hogy a random kisorsolt pontok között túl sok egymáshoz hasonló beállítás volt, így ezek

mind hasonlóan nagy hibajelet produkáltak. Ennek a problémának az elkerülése érdekében szükség volt egyfajta memóriára az algoritmuson belül, mely megjegyzi a célállapottól egy előre beállított határnál nagyobb távolságú pontokat előállító tárcsa beállításokat és az ahhoz hasonló beállításokat le se teszteli, ezzel időt spórolva. Ezzel a módszerrel a gömbön lévő tesztelendő felszínt egyre inkább csökkentettük, így hamarabb találtunk egy olyan pontot, mely már megfelel kezdőpontnak.
Ennél az algoritmusnál fontos volt, hogy megfelelően válasszuk meg azt a hibajelet, amely fölött már kizárjuk a pont körüli területet, mely területet szintén óvatosan kellett növelni ahhoz, hogy ne fordulhasson elő az, hogy az egész gömböt lefedtük rossz területként. Fontos megjegyezni, hogy a tárcsák tökéletlen és egymástól függő működése miatt nem tudjuk egy az egyben megfeleltetni a mért pontokat (melyeket a már említett egységsugarú gömbön tudunk ábrázolni) a beállított szögekkel (melyeket egy 170 egység oldalú kockában tudunk ábrázolni), de ennek ellenére az egymáshoz hasonló beállítások a tárcsákon egymáshoz hasonló polarizációs állapotot eredményeztek azonos állapotú bemenő fényre, tehát lehetett alkalmazni a kizárásos módszert.

## 4.2. Egyfoton-detektorral való mérés

Az algoritmusok polariméterrel való tesztelése után azokat lemértem a valódi kvantumos kulcsmegosztó-rendszer egy részén is, mely további eszközöket tartalmaz.

### 4.2.1. Aurea összefonódott fotonpár forrás

A kvantumos kulcsmegosztó-rendszer egyik legfontosabb összetevője egy összefonódott fotonpár forrás (4.6. ábra). A tanszéki rendszerben egy az Aurea Technology által készített eszköz található, mely 1550 nm hullámhosszú összefonódott fotonpárokat képes előállítani.
A forrásban található egy pumpáló lézerdióda, melynek hullámhossza 775 nm, és egy periodikusan pólusozott lítium-niobát (PPLN) kristály, mely előállítja az összefönódott fotonpárokat, spontán parametrikus lekonverzióval, melynek angol rövidítése SPDC (Spontaneous Parametric Down-Conversion). Ez az eszköz másodpercenként nagyjából 1-1 millió fotont generál, melyeken 150 ezer koincidenciát mértünk, ami azt jelenti, hogy a két kimenetet rácsatolva a detektor egy-egy bemenetére másodpercenként 150 ezer olyan eset volt, amikor 100 ps-os időintervallumon belül mindkét bemeneten detektált fotont, 1 mW-os pumpáló lézerteljesítmény mellett. A forrás belső hőmérséklete és a benne lévő csillapító állítható, ezekkel a két csatorna fotonszáma és azoknak az aránya szabályozható.


**4.6. ábra.** Aurea összefonódott fotonpár forrás [12]

### 4.2.2. Szupravezető nanohuzalos egyfoton-detektor

A rendszer vevőegységében egy ID281-es szupravezető nanohuzalos egyfoton-detektor (4.7. ábra) található, mely az adatlapja szerint 80%-os detektálási hatásfokkal rendelkezik, melynél a jitter átlagosan 35 ps-os FWHM (Full Width at Half Maximum) és a holtideje 10 ns körüli. A másodpercenkénti sötétbeütések, azaz a detektor saját zajából származó hamis detektálások száma maximum 100. Egy detektáláskor a kiadott feszültségimpulzus szélessége 5 ns-nál szélesebb és 100 mV-nál nagyobb értékű [10]. A detektor detektálási hatásfoka polarizáció függő. A maximumhoz tartozó polarizációs állapot illetve a polarizáció változtatás által okozott hatásfok függvénye nem ismert.

### 4.2.3. Time Controller

A feszültségimpulzusokat egy ID900-as TC (Time Controller, 4.8. ábra) dolgozza fel, melyet csatlakoztatni lehet egy számítógéphez és a saját szoftverén keresztül (vagy programkódból irányítva) megkaphatjuk egy bizonyos időintervallumra az impulzusok számát, a beütések számának változását vagy akár több bemenet között a koincidenciát. Az eszköznek 4 bemenete van, melyekre a detektor 4 kimenetét kötöttük rá.

### 4.2.4. Mérések a detektorral

Az eszközök megismerése és az algoritmusok tesztelése után a valódi rendszeren is lemértem az algoritmusok hatékonyságát. A polariméterrel való mérésnél pontosan meg tudtuk mondani, hogy mennyire tér el a beállított polarizációs állapot a célállapottól, de a detektorral való mérésnél már nem tudjuk követni a fény polarizációs

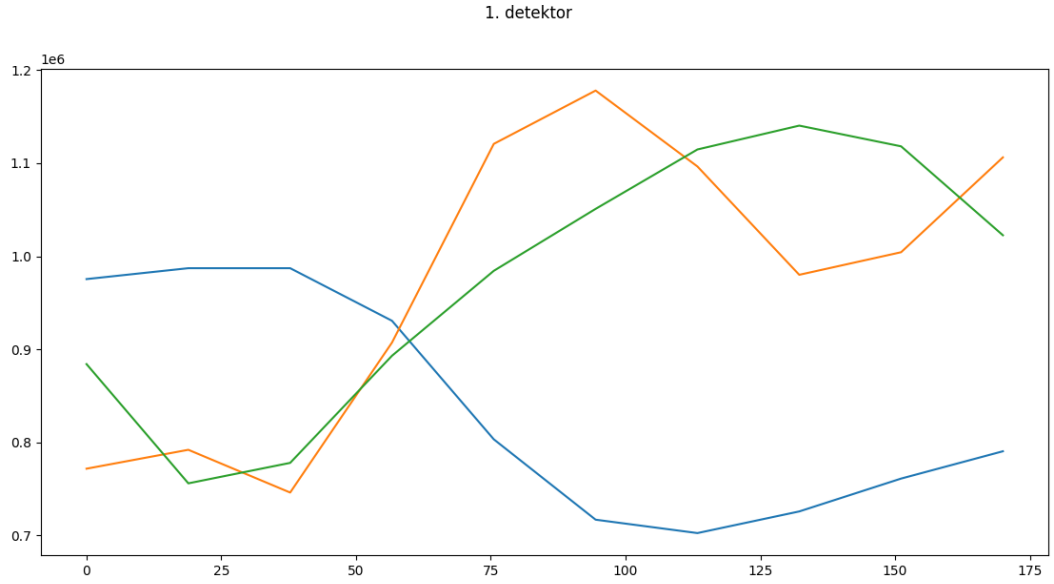
**4.7. ábra.** Szupravezető nanohuzalos egyfoton detektor [10]


**4.8. ábra.** ID900 Time Controller Series [11]

állapotának változását, csak a másodpercenkénti fotonbeütések számát. Az algoritmusok célja a beütések számának maximalizálása.
A rendszer, amin elvégeztem a méréseket, úgy épült fel, hogy az összefonódott fotonforrás mindkét kimenete egy-egy polarizációs osztókockán megy át szabadtérben, mely polarizáció szerint átengedi vagy eltéríti 90 fokkal a fényt, ezután egymódusú optikai szálba becsatolva a detektor egy-egy bemenetére vezetjük a fényt, ezzel valósítva meg azt, hogy megmérjük a foton polarizációját egy bázisban. A detektor első bemenete elé beiktattuk a polarizációkontrollert, tehát az erre jutó fény polarizációját tudjuk aktívan kontrollálni. A négyes bemenetet nem kötöttük be, így azon látszik a sötétbeütések száma.

#### 4.2.4.1. Végigpásztázó algoritmus

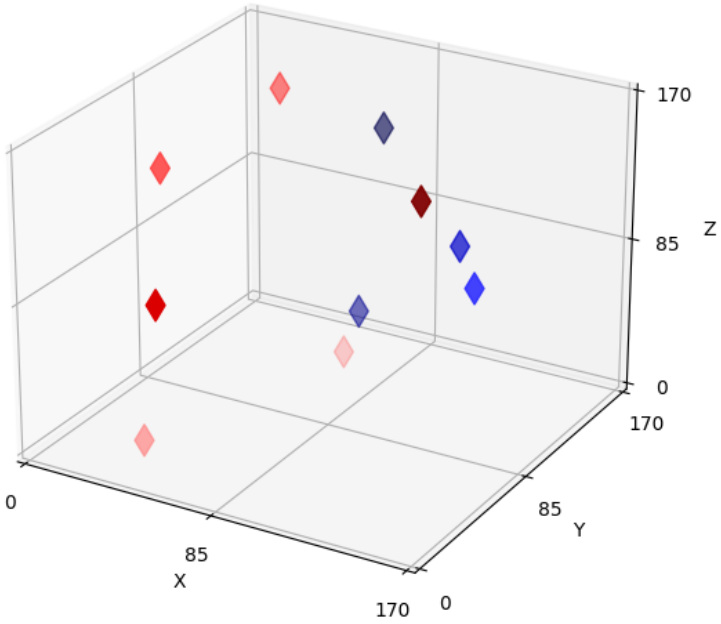
A detektoron elsőként a végigpásztázó algoritmust teszteltem. Az algoritmus átlagosan 1 percig tartott és az átlaghoz képest 15-20%-kal tudta növelni vagy csökkenteni a detektált fotonok számát. Láthatjuk a 4.9. ábrán, hogy a tárcsákat forgatva mennyivel változott meg a detektor első bemenetén detektált fotonok száma. A színek egy-egy tárcsát jelölnek. A diagramról leolvasható, hogy több mint 450 ezer a különbség a detektálás számának maximuma és a minimuma között, tehát lényeges, hogy jól állítsuk be a tárcsákat.




**4.9. ábra.** Végigpásztázó algoritmus hatása az 1. számú detektorbemeneten

#### 4.2.4.2. Random pontok vizsgálata

A 4.10. ábrán és a 4.11. ábrán látható a második algoritmus tesztelése, melyben egy előre megadott számú (10 és 20) random beállításban vizsgáltam a polarizációkontroller hatását a detektor hatásfokára. A pontokat egy kockán ábrázoltam, melynek tengelyei a három tárcsa fokban mérhető elfordítását ábrázolja a vízszintes 0°-hoz képest 0-170 tartományon, mivel a tárcsák is csak ebben a tartományban forgathatók. A pontok színe arányos a mért beütésszámmal, minél pirosabb egy pont, annál több fotont detektált abban a tárcsabeállításban a detektor. Ez az algoritmus, 10 random beállítást vizsgálva, átlagosan 75 másodperc alatt zajlott le és a detektált fotonok számának átlagához képest 20-25%-os növekedést vagy csökkenést tudott okozni.

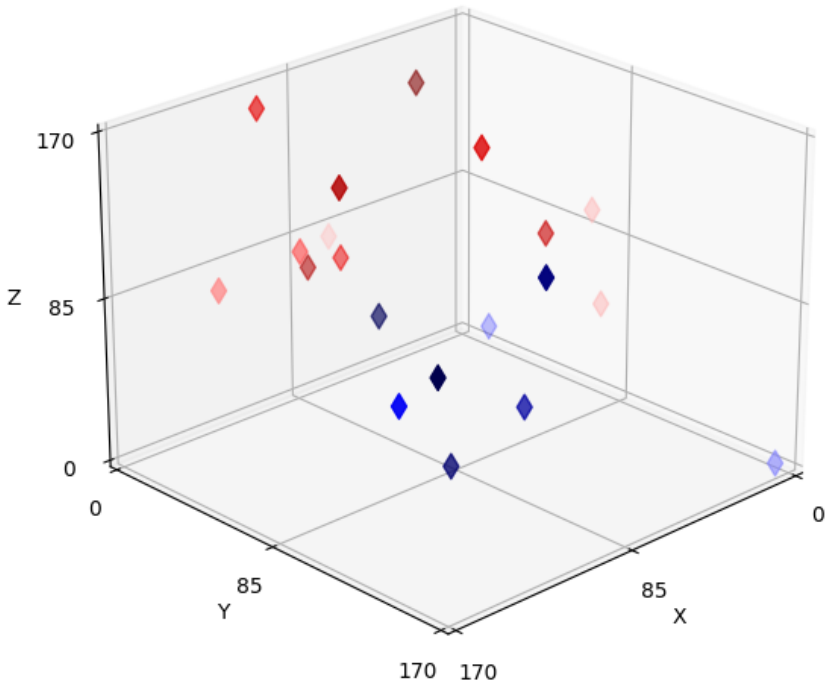



**4.10. ábra.** 10 random pont vizsgálata

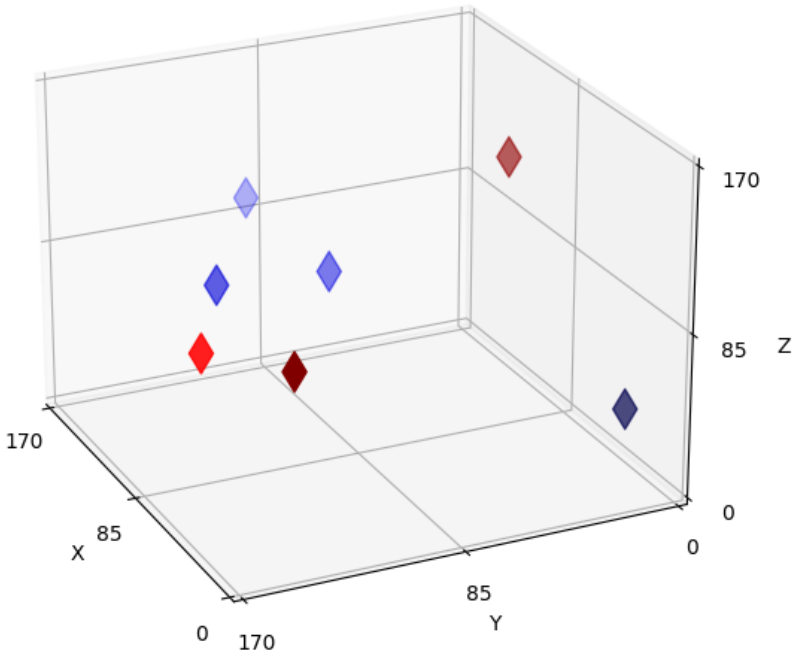
#### 4.2.4.3. Kombinált algoritmus

A kombinált algoritmussal való mérésnél megadtam egy határszámot, mely fölötti beütésszámot mérve már ne keressen további random pontokat, hanem a talált pontból egy kis tartományon (±20° minden tárcsával) futassa le a végigpásztázó algoritmust. Az összefonódott fotonpár forrásnál megfigyelhető volt, hogy nem állandó az általa kibocsátott fotonok száma, hanem időben változott, így a felső határt mindig ehhez kellett igazítani.

A 4.12. ábrán látható mérésnél ez a határ 1 100 000 foton volt másodpercenként. A random pontok közül abban a pontban, amikor a detektálások száma ezt a határt átlépte, a beütésszám 1 109 506 volt. Ebből a pontból indult a végigpásztázó algoritmus, mely a beállításokat finomította úgy, hogy a beütésszám 1 160 539-re nőjön.




**4.11. ábra.** 20 random pont vizsgálata




**4.12. ábra.** Kombinált algoritmus random pontjai

# 5. fejezet

# Összegzés és továbbfejlesztési lehetőségek

A fény polarizációs állapotát és az ezt manipulálni képes eszközök matematikai leírásait megismerve modellezni tudtunk egy eszközt, melynek ideális és hibás működését is szimuláltuk többfajta bemenő polarizációs állapotra. Megállapítottuk, hogy amennyiben mindhárom lemez működik, nem feltétlenül kell ideálisan $\lambda/2$-es és $\lambda/4$-es lemezeknek lenniük ahhoz, hogy bármilyen polarizációs állapototot el tudjunk érni egy tetszőleges bemeneti fényt kontrollálva. Amennyiben viszont az egyik lemez egyáltalán nem forgat fázist és a másik kettő lemez is hibás, akkor előfordulhatnak olyan polarizációs állapotok, amelyeket nem tudunk elérni bizonyos bemenő fényállapotokból.

A polarizációkontroller tesztelése során megállapítottuk, hogy az egyes tárcsák nem feleltethetőek meg ideális $\lambda/2$-es és $\lambda/4$-es lemezeknek, viszont mindhárom tárcsa forgatásával tudjuk változtatni a fény polarizációs állapotát. A tökéletlenségek ellenére is be tudtunk állítani tetszőleges polarizációs állapotot a hatásfok javításához kellő pontossággal tetszőleges bemenő fényből.

A kívánt polarizációs állapot elérésének pontosságát és az ezt megvalósító algoritmusok gyorsaságát először egy olyan rendszerben teszteltük, melyben mérni tudtuk a már kontrollált fény polarizációs állapotát. A tesztelések során megfigyeltük az algoritmusok előnyeit és hátrányait, és azokat ezek alapján továbbfejlesztettük.

Az algoritmusokkal ezután egy kvantumos kulcsmegosztó-rendszer egy részén méréseket végeztünk, melyben megállapíthattuk, hogy a polarizációkontroller valóban tudja növelni az egyfoton-detektor detektálási hatásfokát, mellyel a későbbi kulcsmegosztás sebessége is növelhető.

A továbbiakban még sok fajta fejlesztést végezhetünk az algoritmusokon, a programkódon és a rendszeren is. Az algoritmusok megalkotása során felmerültek egyéb megoldási lehetőségek, mint például a gradiens módszer, mely közvetlenül nem alkal-

mazható, mert nem ismert a detektálási hatásfok polarizációfüggésének függvénye, így a parciális deriváltakat se tudjuk kiszámítani, de azokat tudjuk közelíteni kis mérésekkel. A meglévő algoritmusokat is tovább lehet finomítani a bennük lévő paraméterek automatikus menet közbeni becslésével és változtatásával. A megírt vezérlő programkódot általánosítani lehetne, hogy bármilyen hibajel képzéssel tudjon működni, így elősegítve az eszköz más rendszerekbe való integrálását. További fejlesztési lehetőség lenne a szimulációs program és a vezérlő program egybeépítése és azoknak közös grafikus felhasználói felület készítése, melyben a szimuláció és a mérés összehasonlítható. A kvantumos kulcsmegosztó-rendszerben lévő detektorok mindegyik bemenete elé kell egy ilyen polarizációkontroller, melyeknek meg kell valósítani az időzíthető, összehangolt és automatikus működést.

# Köszönetnyilvánítás

A kutatás a Kulturális és Innovációs Minisztérium Nemzeti Kutatási Fejlesztési és Innovációs Alapból nyújtott támogatásával, a 2022-2.1.1-NL-2022-00004 számú projekt finanszírozásában valósult meg.

# Irodalomjegyzék


[1] R Andrews – A T Joseph – E R Pike – Sarben Sarkar: Control of photon correlations in type II parametric down-conversion. *Journal of Optics B: Quantum and Semiclassical Optics*, 7. évf. (2005. november) 12. sz., S480–S483. p. URL https://doi.org/10.1088/1464-4266/7/12/007.

[2] S. Castelletto – I. P. Degiovanni – M. L. Rastello: Modified Wigner inequality for secure quantum-key distribution. *Phys. Rev. A*, 67. évf. (2003. Apr), 044303. p. URL https://link.aps.org/doi/10.1103/PhysRevA.67.044303. 4 p.

[3] Edward Collett: *Field Guide to Polarization*. 2005. szeptember, SPIE. URL https://doi.org/10.1117/3.626141.

[4] Laszlo Gyongyosi – Laszlo Bacsardi – Sandor Imre: A survey on quantum key distribution. *Infocommunications journal*, 2019. évf. (2019) 2. sz., 14–21. p. URL https://doi.org/10.36244/icj.2019.2.2.

[5] Quantum Information Portal – Wiki: Qubit. URL https://www.quantiki.org/wiki/qubit. Utolsó elérés: 2023.10.27.

[6] Leilei Li – Hengji Li – Chaoyang Li – Xiubo Chen – Yan Chang – Yuguang Yang – Jian Li: The security analysis of e91 protocol in collective-rotation noise channel. *International Journal of Distributed Sensor Networks*, 14. évf. (2018. május) 5. sz., 155014771877819. p. URL https://doi.org/10.1177/1550147718778192.

[7] Angol nyelvű Wikipédia: Jones calculus. URL https://en.wikipedia.org/wiki/Jones_calculus. Utolsó elérés: 2023.10.27.

[8] Angol nyelvű Wikipédia: Rsa (cryptosystem). URL https://en.wikipedia.org/wiki/RSA_(cryptosystem)#Key_size. Utolsó elérés: 2023.10.27.

[9] Angol nyelvű Wikipédia: Shor's algorithm. URL https://en.wikipedia.org/wiki/Shor%27s_algorithm. Utolsó elérés: 2023.10.27.

[10] ID Quantique: ID281 Superconducting Nanowire Series. URL https://www.idquantique.com/quantum-sensing/products/id281-snspd-series/. Utolsó elérés: 2023.10.27.

[11] ID Quantique: ID900 Time Controller Series. URL https://www.idquantique.com/quantum-sensing/products/id900-time-controller/. Utolsó elérés: 2023.10.27.

[12] Auréa Technology: Twin Photon Source at telecom wavelengths. URL https://www.aureatechnology.com/en/products/twin-photons-source.html. Utolsó elérés: 2023.10.27.

[13] Thorlabs: Motorized Fiber Polarization Controllers. URL https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=12896. Utolsó elérés: 2023.10.27.

[14] Thorlabs: Polarimeter Systems with High Dynamic Range. URL https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=1564. Utolsó elérés: 2023.10.27.