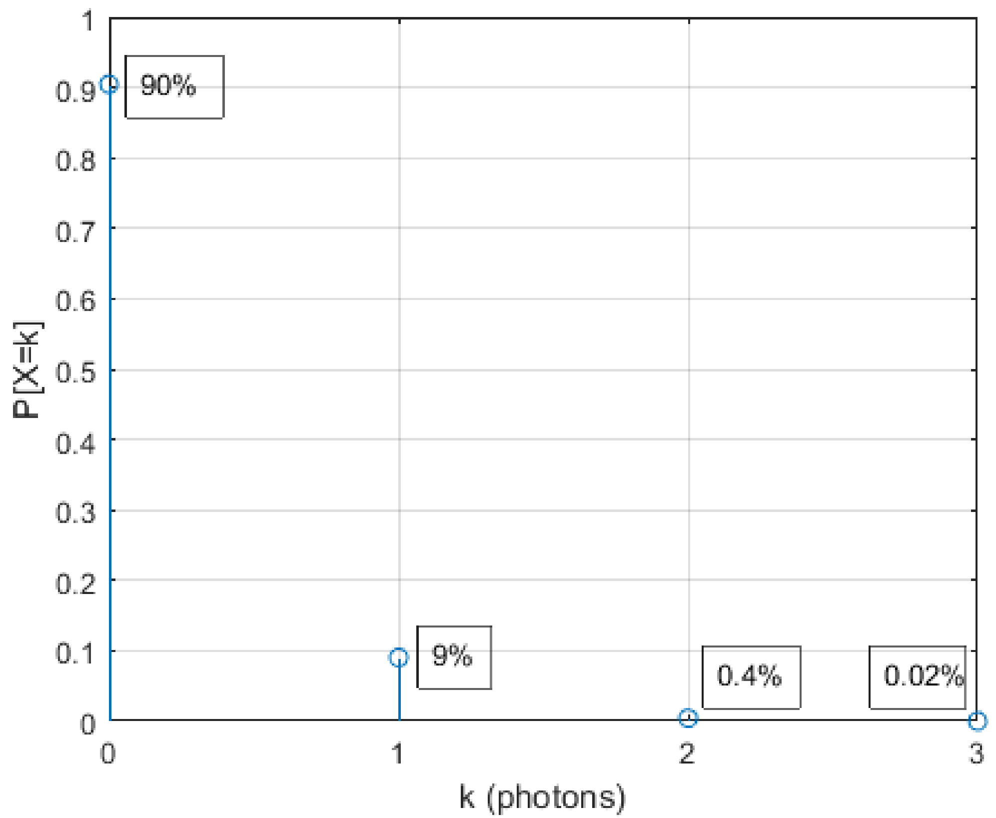
PRACTICAL QUANTUM KEY DISTRIBUTION (QKD)

Photon Counting Module



Probability density function Pr[X=k], with λ equal to 0.1

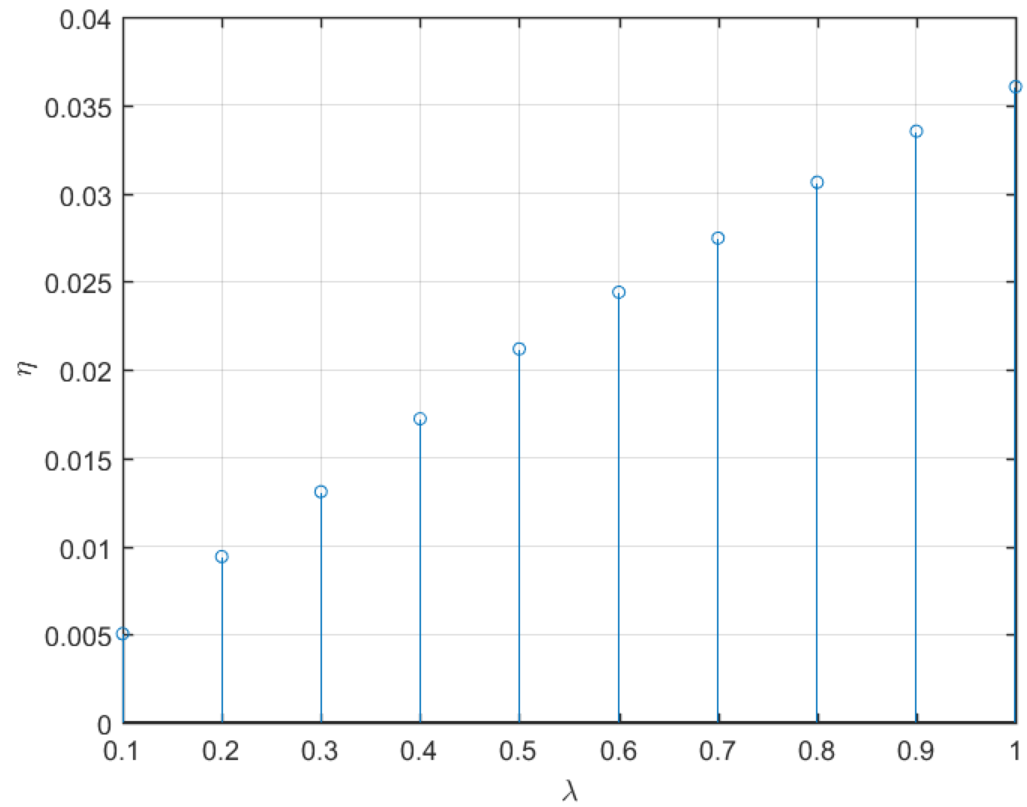
Decoy protocol simulation

Normal operation

```
>> lambda=1;

>> n=5;

>> % generate n random k-photon pulses
>> k=poissrnd(lambda,1,n)

k =

     1     2     3     0     2

eta=0.1;

y0=0.01;

>> % detection probability
>> y=y0+ 1-(1-eta).^k

y =

    0.1100    0.2000    0.2810    0.0100    0.2000

>> % generate n random numbers in the interval (0,1)
>> r=rand(1,n)

r =

    0.3127    0.1615    0.1788    0.4229    0.0942

>> % measure the gain
>> G=sum(r<=y)/n

G =

    0.600

>> % using measured gain, determine quantum efficiency
>> e1=-log(1+y0-G)/lambda
e1 =

    0.89160
```

Attack Simulation

```
>> % find indices of single-photon pulses
i=find(k==1)

i =

     2     5

>> % switch single photon pulses to null
k(i)=0

k =

     0     0     2     0     0

>> % find indices of non null-photon pulses
i=find(k)

i =

     3

>> % switch single photon pulses to null
k(i)=k(i)-1

k =

     0     0     1     0     0
```



Measured quantum efficiency ηas a function of parameter λ when a PNS attack is perpetrated