

Title: Dealing with Photon Loss and Dark Counts in Quantum Key Distribution

Date: Mar 09, 2005 04:05 PM

URL: <http://pirsa.org/05030103>

Abstract:

How to deal with photon loss and
dark currents in QKD:

How to deal with photon loss and
dark currents in QKD:

- A. What is QKD + motivation
- B. Improve well-known
- C. Exotic QKD based error code.

A - encode a random key
Alice → using quantum
state

Bob

A - encode a random key
Alice → using quantum state → Bob
Eve

A - encode a random key
Alice → using quantum state → Bob

Eve induces error ⇒ detectable

A - encode a random key
Alice → using quantum state → Bob

Eve induces error ⇒ detectable
Security is based on laws
of quantum mechanics

Problem: experimental errors
Solution: error correction

Problem: experimental errors
Solution: error correction
Principal: Photon + dark counts

Problem: experimental errors

Solution: error correction

Principal: Photons + dark counts
Source frame

Previous security proof: All are causal



B- BB84

مستقبل
 $\{ |0\rangle, |1\rangle \}$
 $\{ |+\rangle, |-\rangle \}$

B5



$\{ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \}$
 $\{ |+\rangle, |-\rangle \}$

B- BB84

$\{ |0\rangle, |1\rangle \}$
 $\{ |+\rangle, |-\rangle \}$

BB



$\{ |0\rangle, |1\rangle, |+\rangle, |-\rangle \}$
 $\{ |0\rangle, |1\rangle, |+\rangle, |-\rangle \}$



B- BB84

$$\text{Alice } \{ |0\rangle, |1\rangle \}$$

$$\{ |+\rangle, |-\rangle \}$$

Sic- ~~state~~ protocol

$$+ \{ |0\rangle + i|1\rangle, |0\rangle - i|1\rangle \}$$

Bob

$$\{ \frac{1}{\sqrt{2}}|0\rangle, \frac{1}{\sqrt{2}}|1\rangle, \frac{1}{\sqrt{2}}|+\rangle, \frac{1}{\sqrt{2}}|-\rangle \}$$

B92

Alu

$\{14, 3, 14, 3\}$

$\langle 4, 14, 3 \rangle \neq 0$

Bob

{

B92

Alice

$$\{14, 7, 14\}$$

$$\langle 4, 14 \rangle \neq 0$$

Bob

$$\{14, 7, 14\}$$

B92

Alib

$$\{ |4_1\rangle, |4_2\rangle \}$$
$$\langle 4_1, |4_2\rangle \neq 0$$

PBCOO

$$\{ |4_1\rangle, |4_2\rangle \}$$
$$\{ |4_2\rangle, |4_3\rangle \}$$
$$\{ |4_3\rangle, |4_1\rangle \}$$

Bob

$$\{ |4_1\rangle, |4_2\rangle, |4_3\rangle \}$$

$$\{ |4_1\rangle, |4_2\rangle, |4_3\rangle \}$$

$$\{ |4_1\rangle, |4_2\rangle, |4_3\rangle \}$$
$$\{ |4_3\rangle, |4_1\rangle \}$$

EDP

Alice and Bob share

n pairs $|00\rangle + |11\rangle$
entangled

EDP

Alice and Bob share

in pairs $|00\rangle + |11\rangle$
(entangled)

$|01\rangle + |10\rangle$
 $|01\rangle - |10\rangle$
 $|00\rangle - |11\rangle$

we

EDP

Alice and Bob share

n pairs $|00\rangle + |11\rangle$
(entangled)

we can create an entangled pair
 $|00\rangle + |11\rangle$

$|00\rangle + |11\rangle$
 $|01\rangle + |10\rangle$
 $|00\rangle - |11\rangle$

EDP

Alice and Bob share

pairs $|00\rangle + |11\rangle$
(errors)

use error correction on perfect pairs
 $|00\rangle + |11\rangle$

$$\begin{aligned} &|01\rangle + |10\rangle \\ &|01\rangle - |10\rangle \\ &|00\rangle - |11\rangle \end{aligned} \quad \left. \vphantom{\begin{aligned} &|01\rangle + |10\rangle \\ &|01\rangle - |10\rangle \\ &|00\rangle - |11\rangle \end{aligned}} \right] \quad \left. \vphantom{\begin{aligned} &|01\rangle + |10\rangle \\ &|01\rangle - |10\rangle \\ &|00\rangle - |11\rangle \end{aligned}} \right]$$

Key generation = P_e

EDP

Alice and Bob share

n pairs $|00\rangle + |11\rangle$
(entangled)

we can create an perfect pairs
 $|00\rangle + |11\rangle$

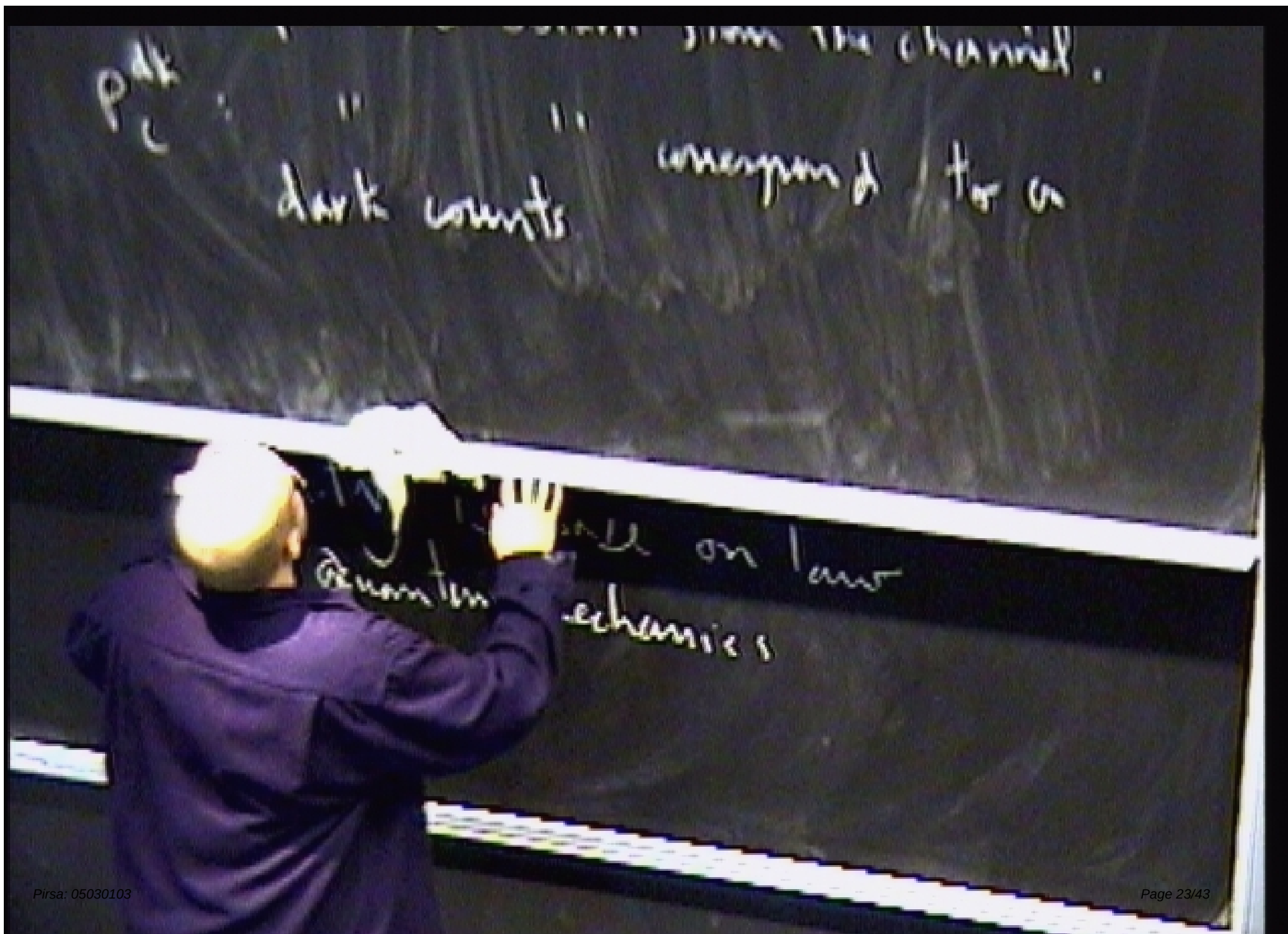
$|00\rangle + |10\rangle$
 $|01\rangle + |10\rangle$
 $|00\rangle + |11\rangle$

Key generation =

$$P_c \frac{M}{n} = P_c [1 - A(b, c)]$$

no error on output

P_c^{sq} : rate of conclusive result of a
successful measurement of a
qubit state obtain from the channel.



P_c^{sq} : rate of conclusive result of a
successful measurement of a
qubit state obtain from the channel.

P_c^{dk} : " " " " " " " " " " " "
dark counts correspond to a

$$P_c = P$$

quantum state obtained from the channel.

p_c^{dk} : " " " " correspond to a dark counts

$$P_c = p_c^{sq} + p_c^{dk}$$

A - Alice → encode a random key using quantum state → Bob

Eve induces errors ⇒ detectable
security is guaranteed

$$P_c = P_c H(e_x)$$

$$P_c = P_c H(e_x) - p d k_c$$

$$P_c = P_c H(e_x) - p_{dk} - p_{sq}^{sq} \left(H(e_x^{sq}, e_z) \right)$$

$$\begin{aligned}
 \psi &= p_c - p_c H(e_x) - p_d k - p_c^{sq} \left(H(e_x^{sq}, e_z^{sq}) - H(e_x^{sq}) \right) \\
 &= p_c \left(\frac{p_c^{sq}}{p_c} - H(e_x) - \frac{p_c^{sq}}{p_c} \left(H(e_x^{sq}, e_z^{sq}) - H(e_x^{sq}) \right) \right)
 \end{aligned}$$

$$\begin{aligned}
 y &= P_c - P_c H(e_x) - p_d k - P_c^{sa} \left(H(e_x^{sa}, e_x^{sa}) - H(e_x^{sa}) \right) \\
 &= P_c \left(\frac{P_c^{sa}}{P_c} - H(e_x) - \frac{P_c^{sa}}{P_c} \left(H(e_x^{sa}, e_x^{sa}) - H(e_x^{sa}) \right) \right)
 \end{aligned}$$

$$\begin{aligned}
 &= P_c - P_c H(e_x) - p_d k - P_c^{sq} \left(H(e_x^{sq}, e_r^{sq}) - H(e_x^{sq}) \right) \\
 &= P_c \left(\frac{P_c^{sq}}{P_c} - H(e_x) - \frac{P_c^{sq}}{P_c} \left(H(e_x^{sq}, e_r^{sq}) - H(e_x^{sq}) \right) \right) \\
 e_x &= \frac{P_c^{sq} e_r^{sq} + P_c^{sk} e_x^{sk}}{P_c}
 \end{aligned}$$

$$P_c^{at} = 0$$

Final threshold:

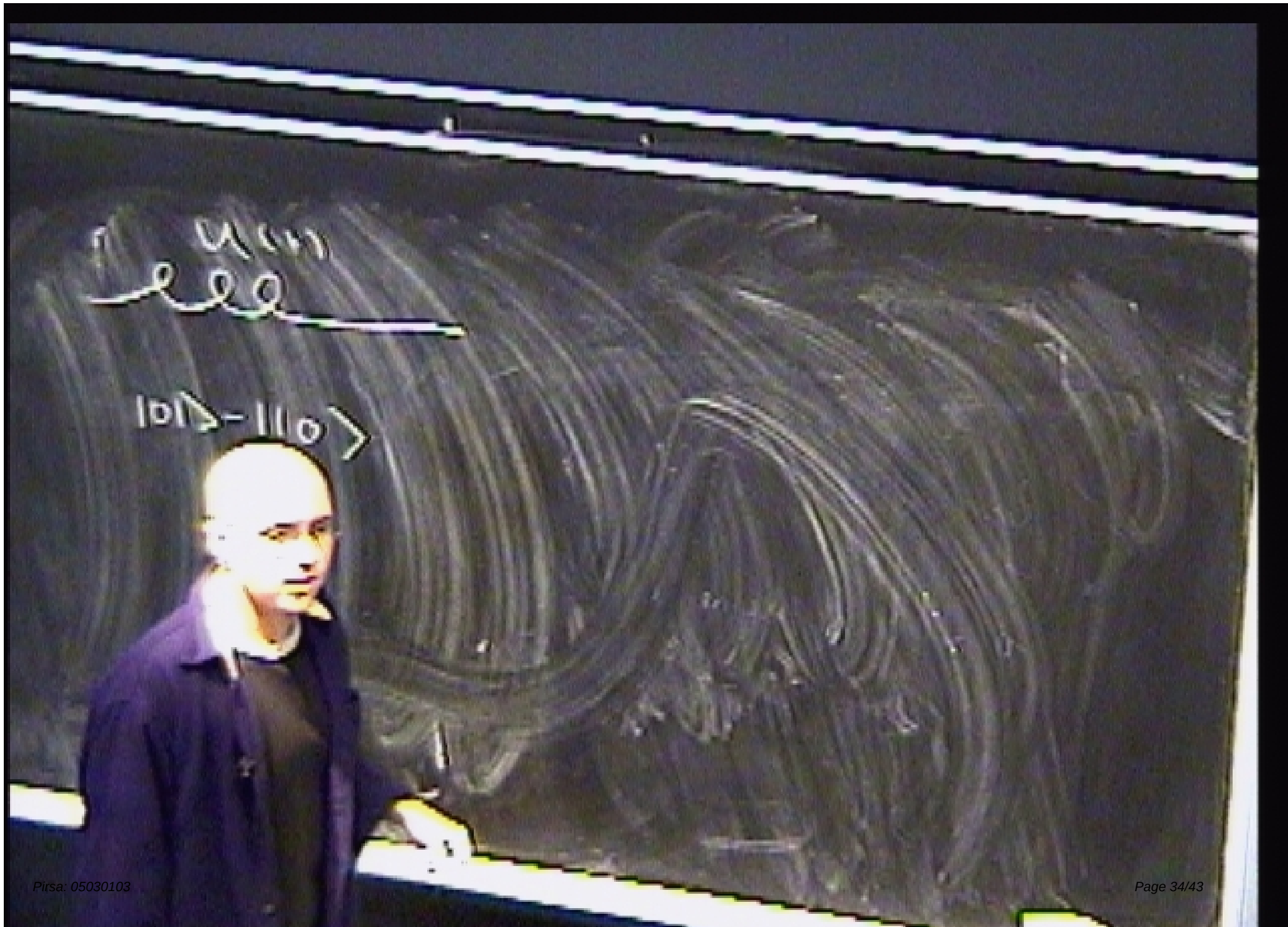
$$P_c^{AP} = 0$$

$$P_c =$$

BB84 : 11,0 %

Sec-State : 12,6 %

PB600 : 9,81 %



$u(0)$

$|0\rangle - |1\rangle$

DFS $u^{\otimes 4}$

$$|0\rangle = \frac{1}{\sqrt{2}} (|a\rangle - |b\rangle)$$

$$|1\rangle = \frac{1}{\sqrt{6}} (|c\rangle - |a\rangle - |b\rangle)$$

$U(1)$
 $U(1)$

$$|a\rangle = |0110\rangle + |1001\rangle$$

$$|b\rangle = |1010\rangle + |1101\rangle \text{ DFS}$$

$U^{\otimes 4}$

$$|c\rangle = |0011\rangle + |1100\rangle$$

$$|\bar{0}\rangle = \frac{1}{\sqrt{2}}(|a\rangle - |b\rangle)$$

$$|\bar{1}\rangle = \frac{1}{\sqrt{6}}(|c\rangle - |a\rangle - |b\rangle)$$

$$|01\rangle = |10\rangle$$

$$|4_1\rangle = |\bar{0}\rangle =$$

$$|4_2\rangle = \frac{1}{2}|\bar{0}\rangle + \frac{\sqrt{3}}{2}|\bar{1}\rangle =$$

$$|4_3\rangle = \frac{1}{2}|\bar{0}\rangle - \frac{\sqrt{3}}{2}|\bar{1}\rangle =$$

$u^{\otimes 4}$
 $u^{\otimes 4}$

$$|a\rangle = |0110\rangle + |1001\rangle$$

$$|b\rangle = |1010\rangle + |0101\rangle \text{ DFS}$$

$$u^{\otimes 4}$$

$$|c\rangle = |0011\rangle + |1100\rangle$$

$$|0\rangle = \frac{1}{\sqrt{2}} (|a\rangle - |b\rangle)$$

$$|01\rangle - |110\rangle$$

$$|1\rangle = \frac{1}{\sqrt{6}} (|c\rangle - |a\rangle - |b\rangle)$$

$$|4_1\rangle = |0\rangle = \sqrt{1} \sqrt{1}$$

$$|4_2\rangle = \frac{1}{2} |0\rangle + \frac{\sqrt{3}}{2} |1\rangle =$$

$$|4_3\rangle = \frac{1}{2} |0\rangle - \frac{\sqrt{3}}{2} |1\rangle = \sqrt{1}$$

$U(1)$
 $U(1)$

$$|a\rangle = |0110\rangle + |1001\rangle$$

$$|b\rangle = |1010\rangle + |0101\rangle \text{ DFS}$$

$U^{\otimes 4}$

$$|c\rangle = |0011\rangle + |1100\rangle$$

$$|\bar{0}\rangle = \frac{1}{\sqrt{2}}(|a\rangle - |b\rangle)$$

$$|\bar{1}\rangle = \frac{1}{\sqrt{6}}(|c\rangle - |a\rangle - |b\rangle)$$

$$|4\rangle = |\bar{0}\rangle = \frac{1}{\sqrt{2}}(|a\rangle - |b\rangle)$$

$$|4_2\rangle = \frac{1}{2}|\bar{0}\rangle + \frac{\sqrt{3}}{2}|\bar{1}\rangle = \frac{1}{2\sqrt{2}}(|a\rangle - |b\rangle) + \frac{\sqrt{3}}{2\sqrt{2}}(|c\rangle - |a\rangle - |b\rangle)$$

$$|4_3\rangle = \frac{1}{2}|\bar{0}\rangle - \frac{\sqrt{3}}{2}|\bar{1}\rangle = \frac{1}{2\sqrt{2}}(|a\rangle - |b\rangle) - \frac{\sqrt{3}}{2\sqrt{2}}(|c\rangle - |a\rangle - |b\rangle)$$

$|a\rangle = |0110\rangle + |1100\rangle$
 $|b\rangle = |1010\rangle + |1101\rangle$ DFS $U^{\otimes 4}$
 $|c\rangle = |1001\rangle + |1100\rangle$
 $|0\rangle = \frac{1}{\sqrt{2}}(|a\rangle - |b\rangle)$
 $|1\rangle = \frac{1}{\sqrt{6}}(|c\rangle - |a\rangle - |b\rangle)$
 $|4_1\rangle = |0\rangle = \sqrt{2}$
 $|4_2\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle = \sqrt{2}$
 $|4_3\rangle = \frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle = \sqrt{2}$

u(11)
uu

$$|a\rangle = |0110\rangle + |1001\rangle$$

$$|b\rangle = |1010\rangle + |0101\rangle \text{ DFS}$$

$$u^{\otimes 4}$$

$$|c\rangle = |0011\rangle + |1100\rangle$$

$$|0\rangle = \frac{1}{\sqrt{2}}(|a\rangle - |b\rangle)$$

$$|01\rangle - |10\rangle$$

$$|1\rangle = \frac{1}{\sqrt{6}}(|c\rangle - |a\rangle - |b\rangle)$$

$$|4_1\rangle = |0\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

$$|4_2\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle = \frac{1}{2}\sqrt{2}$$

$$|4_3\rangle = \frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle = \frac{1}{2}\sqrt{2}$$

$P_{DFS} \{ 1 \times 10^6, 10^6, 10^6, 10^6, \dots \}$

B^+

$P_{DFS} \left\{ \cancel{1000}, \cancel{1001}, \dots \right\}, \quad \mathcal{N} = \{0000, 0001, 0010, \text{etc}\}$

$$B^{\otimes 4} \left(B^{\otimes 4} P B^{\otimes 4} \right) = \left(\begin{array}{c|c} \boxed{\text{1}} & \boxed{\text{0}} \\ \hline \boxed{\text{0}} & \boxed{\text{0}} \end{array} \right)$$



$$O\left(\frac{c}{n}\right)$$

$$O\left(\frac{c^2}{n^2}\right)$$