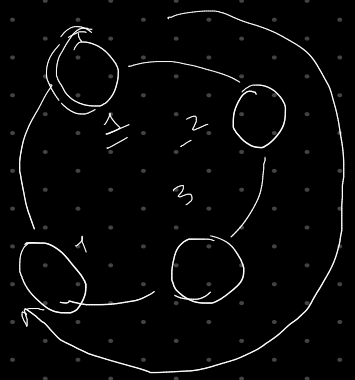
Permutation

Classical $e = [\phi_1\ \phi_2 \cdots \phi_n]$

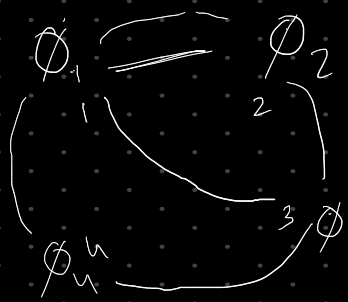
$n!$

$|\psi_0\rangle \rightarrow$

$|\phi_1\rangle|\phi_2\rangle \rightarrow \left(\frac{|\phi_1\rangle|\phi_2\rangle + |\phi_2\rangle|\phi_1\rangle}{\sqrt{2}}\right)$



$\hat{O}_4$: $1 \rightarrow 2$, $2 \rightarrow 3$, $3 \rightarrow 4$, $4 \rightarrow 1$



$\hat{O}_3$: $1 \rightarrow 3$, $3 \rightarrow 2$, $2 \rightarrow 1$

$\hat{O}_2$: $1 \rightarrow 2$, $2 \rightarrow 1$

8436

$P_1 = 0.8$ $P_2 = 0.04$

$|+\rangle |\phi_1\rangle|\phi_2\rangle$

$|0\rangle|\phi_1\rangle|\phi_2\rangle + |1\rangle|\phi_2\rangle|\phi_1\rangle$

$(|\phi_1\rangle|\phi_2\rangle + |\phi_2\rangle|\phi_1\rangle)|0\rangle$

$\hat{O}_n^R$ $R \in \{0, n-1\}$

$R \in \{0, \cdots n-22\}$

$\hat{O}_{n-1}^R$

$|0\rangle$ — H — $|\phi_1\rangle$ — x — $|\phi_1\rangle$

$|\phi_2\rangle$ — x — $|\phi_2\rangle$

$|\phi_1\rangle \rightarrow \left(\sqrt{\pi(\phi_1)}\,|1\rangle + \sqrt{1-\pi(\phi_1)}\,|0\rangle\right)$

$|\phi_1\rangle : \pi(0) + e^{i\pi(\phi_1)}|1\rangle$

$\hat{P} = \sum \prod_i \hat{O}_i^{R_i}$ ← sum has $n!$ terms

$R_i \in \{0, \cdots i-1\}$

$\frac{1}{(1+e^{i\phi})^{i+}}\left(|0\rangle + \cdots + e^{i\phi}|1\rangle\right)$

$n' >> 2^n$

$|\phi_1\rangle|\phi_2\rangle \cdots \to |\phi_0\rangle$

$\bigotimes_{i=1}^{n} |\phi_i\rangle$

$\langle R|$ $\sum_{\{|R\rangle\}}$ $\left(\hat{P}_R |\psi_0\rangle\right)$ (n) — Same superposition

$(0,1)$ $(00,01,10)$

$|R_2\rangle |R_3\rangle \cdots |R_n\rangle$ $n!$

n different terms

$|\phi_1\rangle|\phi_2\rangle \cdots$

$|\phi_2\rangle|\phi_1\rangle \cdots$

$\hat{P} = \hat{O}_2^{R_2} \hat{O}_3^{R_3} \cdots \hat{O}_n^{R_n}$

$\sum_{R_2 R_3 \cdots R_n}$

$= \sum_{R_2=0,1}$ $\hat{O}_2^{R_2} |\psi_0\rangle |R_2 \cdots\rangle$

$R_j \leftarrow \underbrace{0 \cdots j-1}_{\lceil \log(j-1) \rceil}$

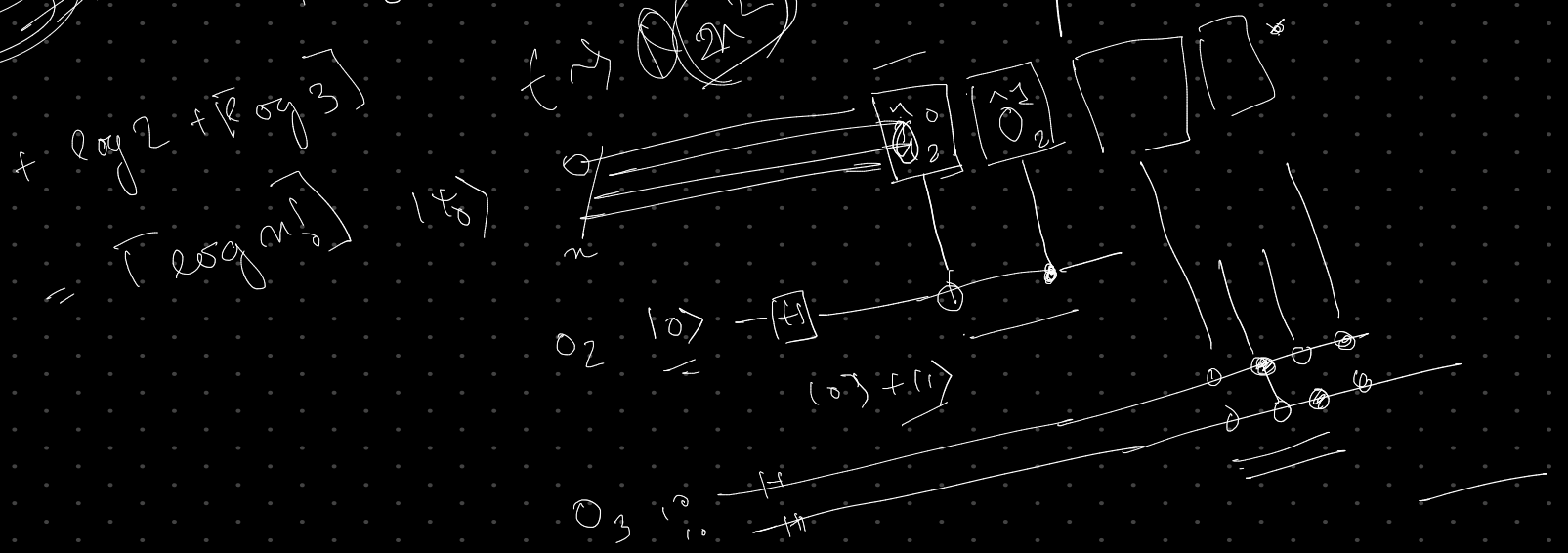
$|\phi_1\rangle|\phi_2\rangle + |\phi_2\rangle|\phi_1\rangle$

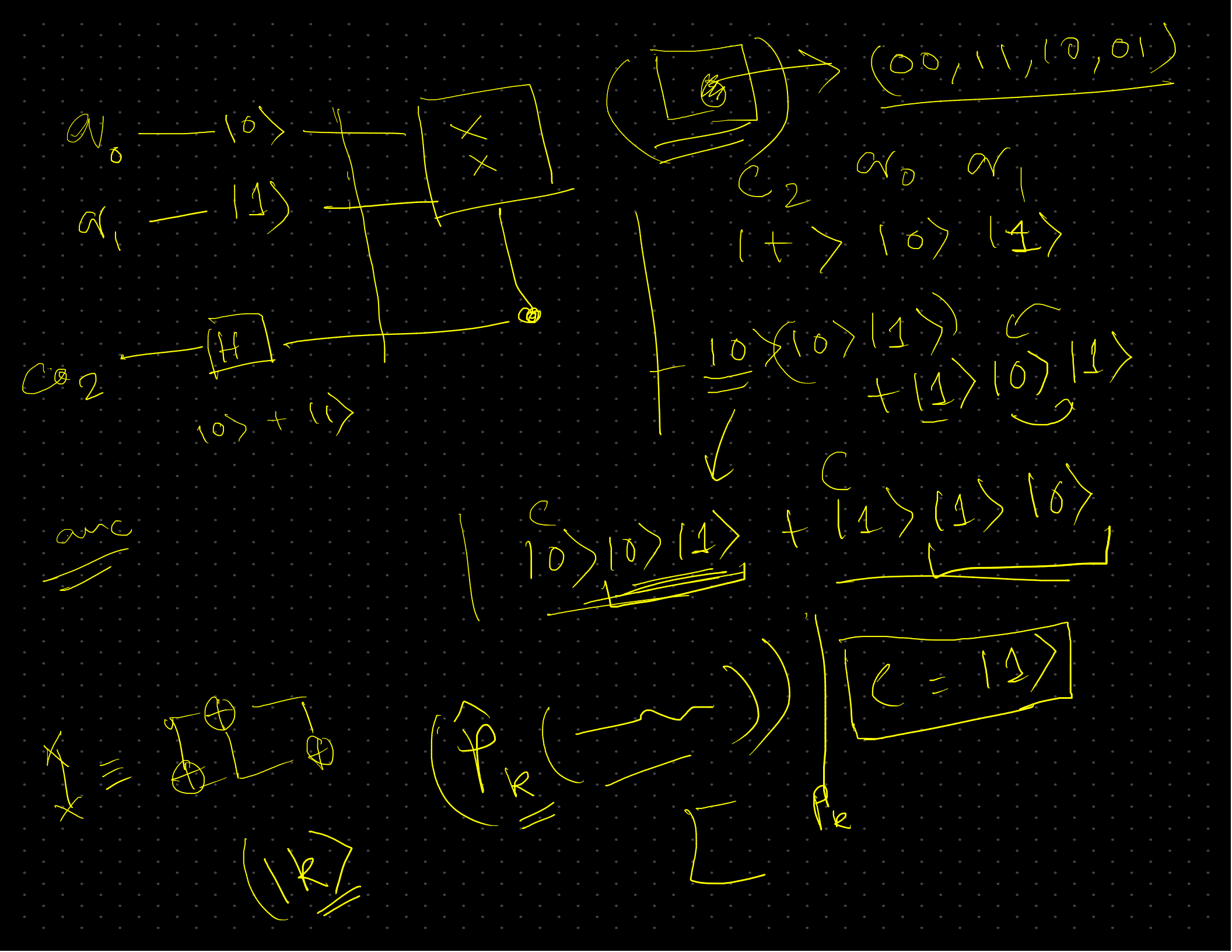
$\log n! \approx n \log n$

$(n) + \log 2 + \lceil \log 3 \rceil$

$= \lceil \log n! \rceil$ $|\psi_0\rangle$

(n) $(2n^2)$




q_0 — $|0\rangle$
q_1 — $|1\rangle$
X
X
C_2
H
$|0\rangle + |1\rangle$
$(00, 11, 10, 01)$
C_2 q_0 q_1
$|+\rangle$ $|0\rangle$ $|1\rangle$
$|0\rangle(|0\rangle|1\rangle)$
$+|1\rangle|0\rangle|1\rangle$
$|0\rangle|0\rangle|1\rangle$ + $|1\rangle|1\rangle|0\rangle$
C
C
and
$|1\rangle$
$C = |1\rangle$
ρ_R
ρ_R
$|1_R\rangle$

Alice: $\binom{n}{2} \cdots \binom{n-1}{}$

~~transmi~~ t transmission

$\log(n-1)$

transmission

1 = 3CNOT secure

[$\otimes$] [2 qubit] → $|\phi_2\rangle$

( ) 5 qubit → [$|\phi_1\rangle$, $|\phi_2\rangle$]

Eve: ( ) ~ $\frac{n}{O(\log n!)}$

$O(n \log n)$

$O(3n^3)$

[ ]

$\log n! \approx n \log n - n$

$n + \log 2 + \log 3$

$n + \log(n!)$

$$\sum_{|R\rangle} |P(R)\rangle\langle\tilde{k}|$$

$$\langle\tilde{k}|R\rangle = \delta_{k\tilde{R}}$$

$$\sum_{|R\rangle} |P(R)\rangle\langle\tilde{k}| \sim |\tilde{k}\rangle$$

non unitary

$$\langle\tilde{k}|\tilde{k}\rangle = \sum_{|R\rangle} |P_k\rangle\langle k|$$

$$\sum_{|R\rangle} \phi(|P_{\tilde{k}}\rangle)\langle k|$$

Ideas !

Eve → player (Eavesdropper)

$|\psi_0\rangle$ ~ init

Encryption Alg

(Encryption key) → 2.

(distributed)

II Equal superposition created

II Spying party chosen

$\hat{P}|\psi_0\rangle$ → completed

x ——— x

Eavesdropper

$(|k_i\rangle)$

x_i

$\lceil \log i \rceil$

$|0\rangle$

$(n) = \frac{1}{3}$ $\lceil \log 3 \rceil$ log 2

$[1, 2, \ldots]$

(k)

$\hat{P}_k \; |\psi_p\rangle \; |k\rangle$

(n)

$|\psi_p\rangle$

$|k\rangle\langle k|$

$|0\rangle\langle 0|$

$(n-1)!$

x_2

$|\psi_k\rangle$

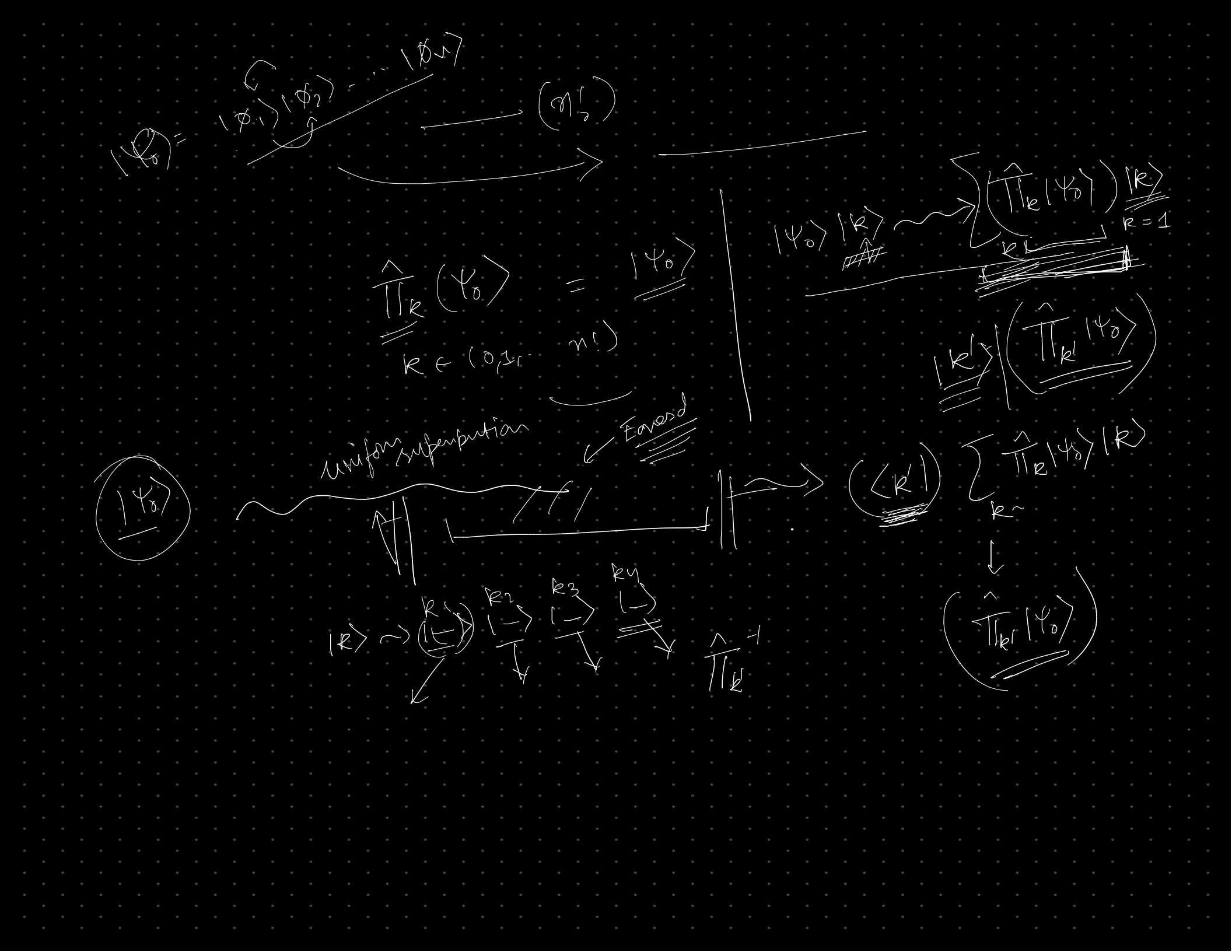
$\left(\frac{n!}{3}\right)$ → Eavesdropper

$x_i \; \forall i$

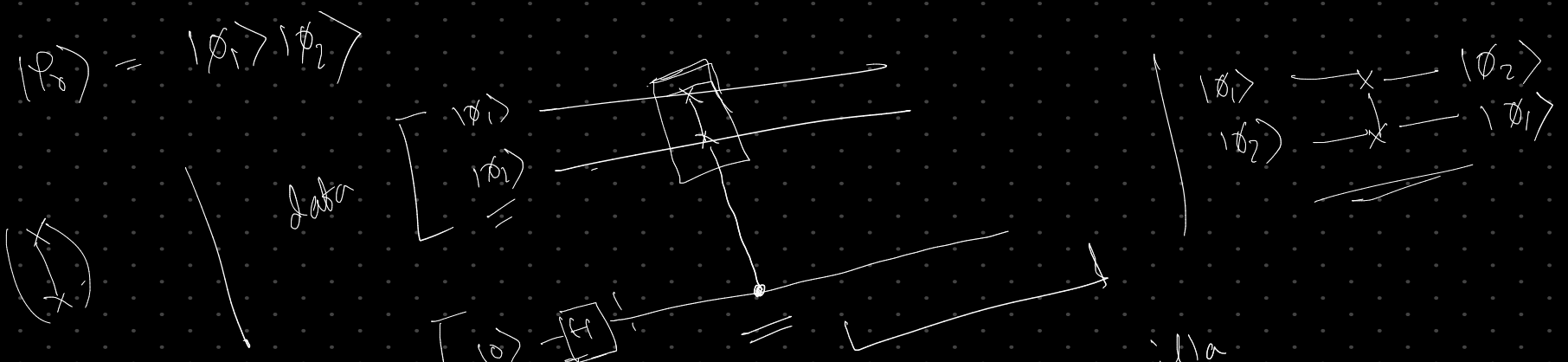
(n)

$\left(\frac{n!}{2}\right)$

(j) →


$|\psi_0\rangle = (|\phi_1\rangle |\phi_2\rangle \cdots |\phi_N\rangle)$
$(n!)$
$\hat{\Pi}_k |\psi_0\rangle = |\psi_0\rangle$
$k \in (0, \ldots n!)$
$|\psi_0\rangle |k\rangle \rightsquigarrow \left(\hat{\Pi}_k |\psi_0\rangle\right) |k\rangle$
$k=1$
$\langle k' | \left(\hat{\Pi}_{k'} |\psi_0\rangle\right)$
$|\psi_0\rangle$
uniform superposition
Favored
$\langle k' | \sum_k \hat{\Pi}_k |\psi_0\rangle |k\rangle$
$|k\rangle \rightsquigarrow$
k_1
k_2
k_3
k_4
$\hat{\Pi}_{k'}^{-1}$
$\hat{\Pi}_{k'} |\psi_0\rangle$

$|\phi_0\rangle = |\phi_1\rangle|\phi_2\rangle$



key $\sim |\phi_1\rangle$

$|\phi_2\rangle|\phi_1\rangle$

$\rightarrow |\phi_1\rangle|\phi_2\rangle(|0\rangle + |1\rangle)$ — ancilla

$\rightarrow |\phi_1\rangle|\phi_2\rangle|0\rangle + |\phi_1\rangle|\phi_2\rangle|1\rangle$

$\rightarrow |\phi_1\rangle(|\phi_2\rangle|0\rangle + |\phi_2\rangle|\phi_1\rangle|1\rangle)$

$(|\phi_2\rangle|\phi_1\rangle)$

$\hat{U} \otimes |1\rangle\langle 1|$

$|\phi_1\rangle|\phi_2\rangle|\phi_3\rangle$

$\hat{T}^2 = 0, 1, 2, 3$

$\hat{U}_3(\psi_0) = |\phi_3\rangle|\phi_1\rangle|\phi_2\rangle$
$|\phi_2\rangle|\phi_3\rangle|\phi_1\rangle$

$|\psi_0\rangle = |\phi_1\rangle|\phi_2\rangle|\phi_3\rangle$

$\hat{U}_3^{(1)}|\psi_0\rangle = |\phi_3\rangle|\phi_1\rangle|\phi_2\rangle$

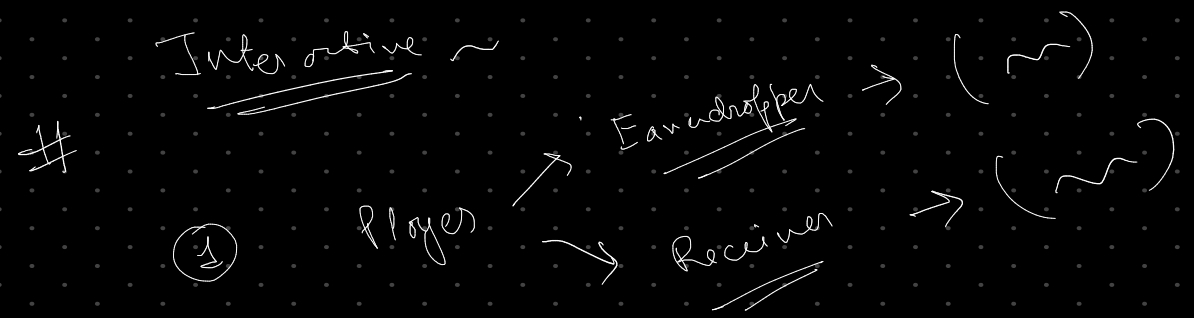
$\hat{U}_3^{(2)}|\psi_0\rangle = - - - -$

$\hat{U}_2|\psi_0\rangle = |\phi_2\rangle|\phi_1\rangle|\phi_3\rangle$

$\hat{U}_3'\hat{U}_2|\psi_0\rangle$

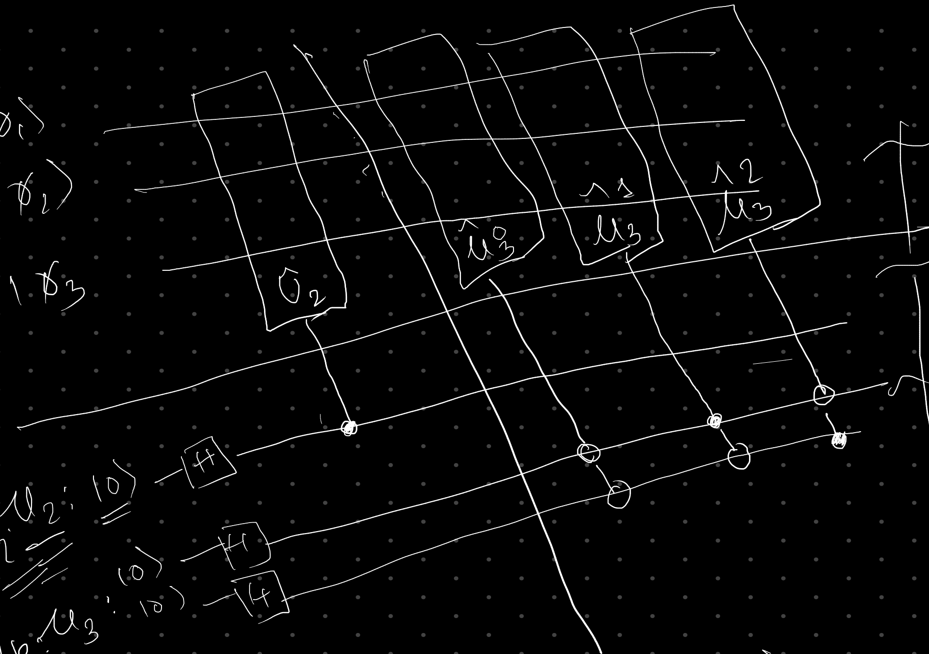
$\hat{U}_3^2\hat{U}_2'|\psi_0\rangle$

$3! = 6$


Interactive
#
1
Player
Eavesdropper
Receiver

$|\psi_0\rangle$ $\left\{ |\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle \right.$

$3 \times 2 = 6$



$|0\rangle + |1\rangle$ $(|\psi_0\rangle)$

U_2

$U_3 \; (|\psi_0\rangle + |\phi_2\rangle|\phi_1\rangle|\phi_3\rangle)$

2^3

$U_2^{0,1}, U_3^{0,1,2}$

$k_2: U_2: |0\rangle$ — H

$k_3: U_3: |0\rangle |0\rangle$ — H, H

$n \sim \lceil \log n \rceil$

(3) keys $\left(\frac{3!}{2}\right)$ (3!)

Code
$k_2 = 0$
$k_3 = (0, 1)$

0 → 00
1 → 01
2 → 10
3 → 11

Alpha

Eve
k_2 (3)

(2) k_2 k_3

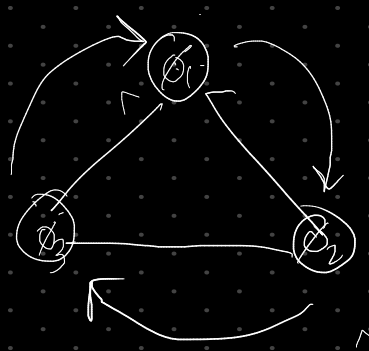
$|\phi_1\rangle |\phi_2\rangle |\phi_3\rangle$

$\hat{P}_2^{\{0,1\}}$

$\tilde{P}_3^{\{0,1,2\}}$

$\hat{P}_2$ $\hat{P}_3$

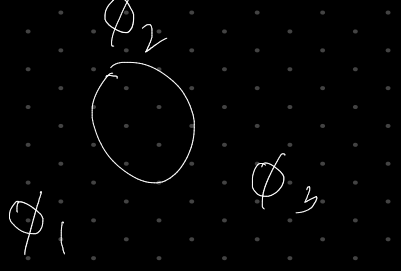
$[\,|\phi_1\rangle\ ,\ |\phi_2\rangle\ ,\ |\phi_3\rangle\,]$



$(\hat{P}_3)^0\ ,\ (\hat{P}_3)^1\ ,\ (\hat{P}_3)^2$

$\hat{P}_3$

P_3^2



$P_2 \in \{0,1\}$ — $b_1 \geq 1$

$P_3 \in \{0,1,2\}$ $(\hat{P}_2)^0$

$b_3 : 00\ ,\ 01\ ,\ 10\ ,\ 11$

$P_n \in \{0,\ldots,n-1\}$

$[\,\phi_1(n-1)\,]$ $(\hat{P}_2)^1$

$n=3$

$j=2$ P_2 ①

$j=3$ P_3

$\underline{5! = 6}$

$(\hat{P}_3)^{\{0,1,2\}}$

$(\hat{P}_3)^{\{0,1,2\}}$

$j \in [\,\phi_1 \quad n+1\,]$

$j \in [2,3,4,\ldots,n+1]$

$m = 4$

$\hat{p}_2^{(0,1)}, \hat{p}_3^{(0,1,2)}, \hat{p}_4^{(0,1,2,3)}$

$\left| \frac{1010}{②} \right| 1001$

$\log_2^3 \simeq 1.3$