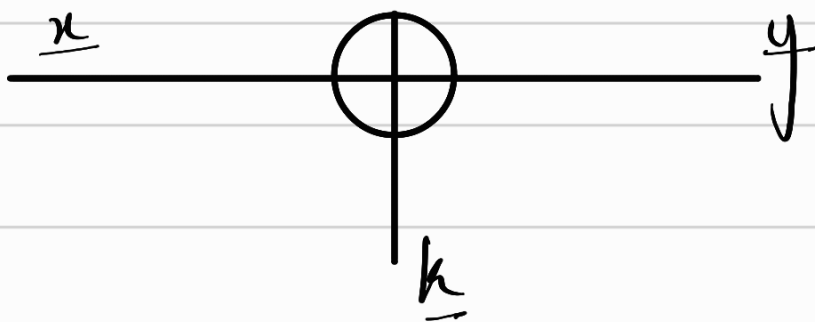


# Quantum Information Theory

## Mid term examination

Solutions by Samarth  
Kashyap

1 (1) One-time padding



$$P(x_i = 0) = p_i \quad P(k_i = 0) = 1/2$$

Since  $x_i$  are independent and so are  $k_i$ , if a cipher is secure for  $n=1$ , it will hold for any  $n$  since  $I(x_i, x_j) = H(x_i) \delta_{ij}$ .

$$P(x=0) = p \quad P(k=0) = 1/2$$

$$P(y=0) = \frac{p}{2} + \frac{1-p}{2} = \frac{1}{2}$$

$$H(y) = 1 \quad H(y|x) = 1$$

$$\Rightarrow I(x; y) = I(y; x) = 0$$

No information is gleaned about the message from cypher text

→ Secure (both cases)

$$(2) \quad p(x = x_i) = p_i \quad i \in \{1, 2, \dots, d\}$$

$$H(x) = - \sum_{i=1}^d p_i \log p_i$$

$$\begin{aligned} \log d - H(x) &= \log d \sum_{i=1}^d p_i - H(x) \\ &= \sum_{i=1}^d p_i \log(d p_i) \end{aligned}$$

Because  $\ln x \geq 1 - \frac{1}{x}$ ,

$$\log x \geq \left(1 - \frac{1}{x}\right) \log c$$

$$\begin{aligned} \log d - H(x) &\geq \sum_{i=1}^d p_i \left(1 - \frac{1}{d p_i}\right) \\ &= \sum_{i=1}^d \left(p_i - \frac{1}{d}\right) \\ &= \sum_{i=1}^d p_i - 1 \end{aligned}$$

$$\log d - H(x) \geq 0$$

$$(1) C = (NO T)_2 = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes X$$

$$X_1 = X \otimes \mathbb{1} \quad Z_1 = Z \otimes \mathbb{1}$$

$$(a) CX_1 = |0\rangle\langle 1| \otimes \mathbb{1} + |1\rangle\langle 0| \otimes X$$

$$CX_1 C = |0\rangle\langle 1| \otimes X + |1\rangle\langle 0| \otimes X$$

$$CX_1 C = X_1 \otimes X_2$$

$$(b) CZ_1 = |0\rangle\langle 0| \otimes \mathbb{1} - |1\rangle\langle 1| \otimes X$$

$$CZ_1 C = |0\rangle\langle 0| \otimes \mathbb{1} - |1\rangle\langle 1| \otimes \mathbb{1}$$

$$CZ_1 C = Z_1$$

(2) Let us write

$$|\psi\rangle = \sum_i \lambda_i |i\rangle_A |i\rangle_B \quad (\text{Schmidt})$$

$$\text{with } \lambda_i \in \mathbb{R}, \lambda_i \geq 0, \sum_i \lambda_i^2 = 1$$

$$\rho = \sum_{ij} \lambda_i \lambda_j |ii\rangle \langle jj|$$

$$\rho_A = \text{Tr}_B \rho = \sum_k \langle k|_B \rho |k\rangle_B$$

$$= \sum_k \lambda_k^2 |k\rangle \langle k|$$

$$\rho_B = \text{Tr}_A \rho = \sum_k \lambda_k^2 |k\rangle \langle k|$$

$$f\left(\sum_k \lambda_k^2 |k\rangle\langle k|\right) = \sum_k f(\lambda_k^2) |k\rangle\langle k|$$

$$\begin{aligned} (f(\rho_A) \otimes \mathbb{1}) |\Psi\rangle &= \left( \sum_k f(\lambda_k^2) |k\rangle\langle k| \otimes \mathbb{1} \right) \\ &\quad \sum_i \lambda_i |ii\rangle \\ &= \sum_i \lambda_i f(\lambda_i^2) |ii\rangle \end{aligned}$$

$$\begin{aligned} (\mathbb{1} \otimes f(\rho_B)) |\Psi\rangle &= \left( \mathbb{1} \otimes \sum_k f(\lambda_k^2) |k\rangle\langle k| \right) \\ &\quad \sum_i \lambda_i |ii\rangle \\ &= \sum_i \lambda_i f(\lambda_i^2) |ii\rangle \end{aligned}$$

$$\therefore (f(\rho_A) \otimes \mathbb{1}) |\Psi\rangle = (\mathbb{1} \otimes f(\rho_B)) |\Psi\rangle$$

3.

$$W_{ij} = \{X(i)Z(j)\}_{i,j \in \{0, \dots, d-1\}}$$

There are  $d^2$  such operators. To show:

$$\frac{1}{d^2} \sum_{x,z} W_{xz} \rho W_{xz}^\dagger = \Pi$$

We can write

$$\frac{1}{d^2} \sum_{x,z} X(x)Z(z) \rho Z^\dagger(z) X^\dagger(x)$$

$$= \frac{1}{d^2} \sum_x X(x) \left( \frac{1}{d} \sum_z Z(z) \rho Z^\dagger(z) \right) X^\dagger(x)$$

We can consider the operation as a composition of  $Z$  and  $X$  gates.

$$U_1(\rho) = \frac{1}{d} \sum_{z=0}^{d-1} Z(z) \rho Z(z)^\dagger$$

Can be simplified using

$$Z(z) = \sum_{j=0}^{d-1} \exp(i2\pi zj/d) |j\rangle \langle j|$$

$$U_1(\rho) = \frac{1}{d} \sum_{z=0}^{d-1} \sum_{j,k=0}^{d-1} \exp(i2\pi z(j-k)/d) \langle j|\rho|k\rangle |j\rangle \langle k|$$

$$= \frac{1}{d} \sum_{j,k} \left[ \sum_{z=0}^{d-1} \exp(i2\pi z(j-k)/d) \right] \langle j|\rho|k\rangle |j\rangle \langle k|$$

$$\text{If } j \neq k, \sum_{z=0}^{d-1} \exp\left(\frac{i2\pi z(j-k)}{d}\right) = 0 \quad (\text{GP sum})$$

$$\therefore U_1(\rho) = \frac{1}{d} \sum_j \langle j|\rho|j\rangle |j\rangle \langle j|$$



Transforming to conjugate basis,

$$\begin{aligned}
 \mathcal{N}_1(\rho) &= \frac{1}{d} \sum_j \langle j | \rho | j \rangle \sum_{m=0}^{d-1} \exp(-i2\pi m j / d) |m\rangle_x \\
 &\quad \sum_{n=0}^{d-1} \exp(i2\pi n j / d) \langle n |_x \\
 &= \frac{1}{d} \sum_{j,m,n} \langle j | \rho | j \rangle \exp(i2\pi n(n-m)j / d) |m\rangle_x \langle n |_x
 \end{aligned}$$

Since  $X(a)$  is the phase operator in conjugate space, it acts to only preserve the diagonal elements:

$$\begin{aligned}
 \mathcal{N}_2 \circ \mathcal{N}_1(\rho) &= \frac{1}{d} \sum_{j,m} \langle j | \rho | j \rangle |m\rangle_x \langle m |_x \\
 &= \frac{1}{d} \sum_j \langle j | \rho | j \rangle \sum_m |m\rangle_x \langle m |_x
 \end{aligned}$$

$$\mathcal{N}_2 \circ \mathcal{N}_1(\rho) = \frac{1}{d} \mathbb{1} = \pi$$

If the randomness of applying  $W$  is from a key, then this functions as a quantum one time pad.

$$4. \mathcal{N}^{A \rightarrow B}(\rho_A) = \sum_j \mathcal{N}_j \rho_A \mathcal{N}_j^\dagger$$

We have the extension

$$\mathcal{U}_N^{A \rightarrow BE} = \sum_j \mathcal{N}_j \otimes |j\rangle^E$$

And the complementary channel

$$\mathcal{N}_c^{A \rightarrow E}(\rho_A) = \text{Tr}_B \left\{ \mathcal{U}_N^{A \rightarrow BE}(\rho_A) \right\}$$

$$\begin{aligned} \mathcal{U}_N^{A \rightarrow BE}(\rho_A) &= \sum_j \mathcal{N}_j \otimes |j\rangle^E \rho_A \sum_k \mathcal{N}_k^\dagger \otimes \langle k|^E \\ &= \sum_{jk} \mathcal{N}_j \rho_A \mathcal{N}_k^\dagger \otimes |j\rangle \langle k|^E \end{aligned}$$

$$\text{Tr}_B(U_{A \rightarrow BE}(\rho))$$

$$= \sum_{j,k} \langle j | U_{A \rightarrow BE} \rho U_k^\dagger | l \rangle^B | j \rangle \langle k |^E$$

$$\rho_E = \sum_{j,k} \text{Tr} \left\{ U_{A \rightarrow BE} \rho U_k^\dagger \right\} | j \rangle \langle k |^E$$

5.

$$\text{Tr}_R(|AR_1\rangle \langle AR_1|) = \rho^A$$

$$\text{Tr}_R(|AR_2\rangle \langle AR_2|) = \rho^A$$

let us write

$$|AR_1\rangle = \sum_i \alpha_i |a_i\rangle |b_i\rangle$$

$$|AR_2\rangle = \sum_i \beta_i |\tilde{a}_i\rangle |\tilde{b}_i\rangle$$

$$\rho^{AR_1} = \sum_{ij} \alpha_i \alpha_j |a_i\rangle \langle a_j| \otimes |b_i\rangle \langle b_j|$$

$$\text{Tr}_R(\rho^{AR_1}) = \sum_i \alpha_i^2 |a_i\rangle \langle a_i|$$

$$\text{Tr}_R(\rho^{AR_2}) = \sum_i \beta_i^2 |\tilde{a}_i\rangle \langle \tilde{a}_i|$$

$$\Rightarrow \alpha_i = \beta_i, \quad |a_i\rangle = |\tilde{a}_i\rangle$$

(since  $\alpha, \beta \in \mathbb{R}$  and  $\{a_i\}, \{\tilde{a}_i\}$  are orthonormal sets)

Since  $\{b_i\}, \{\tilde{b}_i\}$  are orthonormal sets,

we can construct  $U_R$  s.t.

$$|b_i\rangle = U_R |\tilde{b}_i\rangle$$

$$\therefore |AR_1\rangle = (\mathbb{1}_A \otimes U_R) |AR_2\rangle$$

