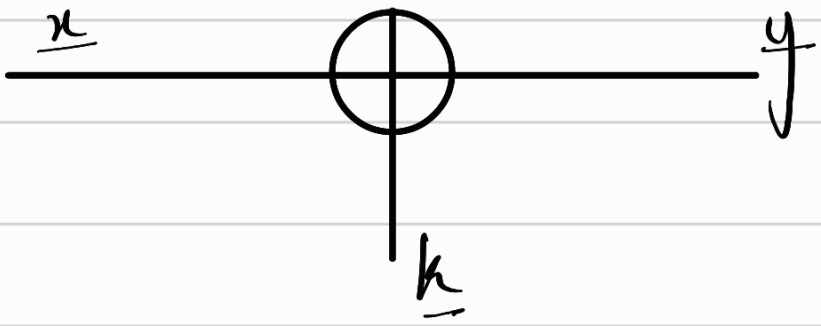
Quantum Information Theory
Mid term examination

Solutions by Samarth Kashyap

1

(i) One-time padding



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

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

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

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

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

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

No information is gleaned about the message from cypher text

→ Secure (both cases)

(2) $p(X = x_i) = p_i \qquad i \in \{1, 2 \ldots d\}$

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

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

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

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

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

$$\log d - H(X) \geq \sum_{i=1}^{d} p_i \left(1 - \frac{1}{d p_i}\right)$$

$$= \sum_{i=1}^{d} \left(p_i - \frac{1}{d}\right)$$

$$= \sum_{i=1}^{d} p_i - 1$$

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

2.

(1) $C = CNOT_{12} = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes X$

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

(a)

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

$$CX_1C = |0\rangle\langle 1| \otimes X + |1\rangle\langle 0| \otimes X$$

$$CX_1C = X_1 \otimes X_2$$

(b)

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

$$CZ_1C = |0\rangle\langle 0| \otimes \mathbb{1} - |1\rangle\langle 1| \otimes \mathbb{1}$$

$$CZ_1C = Z_1$$

(2) Let us write

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

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

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

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

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

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

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

$$\left(f(\rho_A)\otimes \mathbb{1}\right)|\psi\rangle = \left(\sum_k f(\lambda_k^2)|k\rangle\langle k|\otimes \mathbb{1}\right) \sum_i \lambda_i |ii\rangle$$

$$= \sum_i \lambda_i f(\lambda_i^2)|ii\rangle$$

$$\left(\mathbb{1}\otimes f(\rho_B)\right)|\psi\rangle = \left(\mathbb{1}\otimes \sum_k f(\lambda_k^2)|k\rangle\langle k|\right) \sum_i \lambda_i |ii\rangle$$

$$= \sum_i \lambda_i f(\lambda_i^2)|ii\rangle$$

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

3.

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

There are d^2 such operators. To show:

$$\frac{1}{d^2} \sum_{x_2 z_2} W_{x_2 z_2} \rho W_{x_2 z_2}^{\dagger} = \Pi$$

We can write

$$\frac{1}{d^2} \sum_{x_2 z_2} X(x) Z(z_2) \rho Z^{\dagger}(z_2) X^{\dagger}(x)$$

$$= \frac{1}{d^2} \sum_{x} X(x) \frac{1}{d} \sum_{z_2} Z(z_2) \rho Z^{\dagger}(z_2) X^{\dagger}(x)$$

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

$$\mathcal{N}_1(\rho) = \frac{1}{d}\sum_{z=0}^{d-1} Z(z)\,\rho\, Z(z)^\dagger$$

Can be simplified using

$$Z(z) = \sum_{j=0}^{d-1} \exp(i 2\pi z j/d)\,|j\rangle\langle j|$$

to

$$\mathcal{N}_1(\rho) = \frac{1}{d}\sum_{z=0}^{d-1}\sum_{j,k=0}^{d-1} \exp\left(\frac{i 2\pi z}{d}(j-k)\right)\langle j|\rho|k\rangle\, |j\rangle\langle k|$$

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

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

$$\therefore \mathcal{N}_1(\rho) = \frac{1}{d}\sum_j \langle j|\rho|j\rangle\,|j\rangle\langle j|$$

Transforming to conjugate basis,

$$\mathcal{N}_1(\rho) = \frac{1}{d}\sum_j \langle j|\rho|j\rangle \sum_{m=0}^{d-1} \exp\left(-i2\pi mj/d\right)|m\rangle_x$$

$$\sum_{n=0}^{d-1} \exp\left(i2\pi nj/d\right)\langle n|_x$$

$$= \frac{1}{d}\sum_{j,m,n} \langle j|\rho|j\rangle \exp\left(i2\pi(n-m)j/d\right)|m\rangle_x\langle n|_x$$

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

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

$$= \frac{1}{d}\sum_j \langle j|\rho|j\rangle \sum_m |m\rangle_x\langle m|_x$$

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

If the randomness of applying $W_{\alpha z}^{\alpha 2}$ is from a key, then this functions as a quantum one time pad.

4. $$\mathcal{N}^{A\to B}(\rho_A) = \sum_j N_j \rho N_j^\dagger$$

We have the extension

$$U_{\mathcal{N}}^{A\to BE} = \sum_j N_j \otimes |j\rangle^E$$

And the complementary channel

$$\mathcal{N}_c^{A\to E}(\rho_A) = \mathrm{Tr}_B\{U_{\mathcal{N}}^{A\to BE}(\rho_A)\}$$

$$U_{\mathcal{N}}^{A\to BE}(\rho_A) = \sum_j N_j \otimes |j\rangle^E \rho_A \sum_k N_k^\dagger \otimes \langle k|^E$$

$$= \sum_{jk} N_j \rho_A N_k^\dagger \otimes |j\rangle\langle k|^E$$

$$\mathrm{Tr}_B\left(\mathcal{U}_N^{A\to BE}(\rho)\right)$$

$$= \sum_{djk} \langle d|^B N_j \rho N_k^\dagger |d\rangle^B \; |j\rangle\langle k|^E$$

$$\rho_E = \sum_{jk} \mathrm{Tr}\left\{N_j \rho_A N_k^\dagger\right\} \; |j\rangle\langle k|^E$$

5.

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

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

Let us write

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

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

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

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

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

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

(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.

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

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