QuCrypt | Week #3 27 oct 2016

Quantifying Information

§3.1 What it means to be ignorant: the ideal case

§3.1.1

Def^n: Ignorance := consider K (classical info) & E (quantum memory)

(E contains all information Eve has, including intercepted messages)

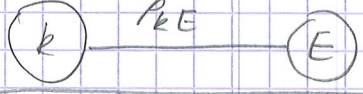
We want ρ_K of ρ_{KE} to be the maximally mixed state; $\rho_K = \frac{\mathbb{1}}{|K|}$ (# keys)

This doesn't mean Eve doesn't know the key

That is ensured if $\rho_{KE} = \rho_K \otimes \rho_E$

i.e. $\mathcal{E}_{KE}(E)$ is ignorant about the key (k)

if $\rho_{KE} = \frac{1}{|K|} \otimes \rho_E$.



e.g. $\rho_{KE} = \frac{1}{2}|0\rangle\langle 0|^K \otimes |+\rangle\langle +|^E + \frac{1}{2}|1\rangle\langle 1| \otimes |+\rangle\langle +|$

$\mathrm{tr}_E(\rho_{KE}) = \rho_K = \frac{\mathbb{1}}{2}$

also, $\rho_{KE} = \frac{\mathbb{1}}{2} \otimes |+\rangle\langle +|^E$

§3.1.2 e.g. 2 $\rho_{KE} = \frac{1}{2}|0\rangle\langle 0|^K \otimes |0\rangle\langle 0|^E + \frac{1}{2}|1\rangle\langle 1|^K \otimes |+\rangle\langle +|^E$

$\mathrm{tr}_E(\rho_{KE}) = \frac{\mathbb{1}}{2}$

e.g. 3 $\rho_{KE} = \frac{1}{3}|0\rangle\langle 0|^K \otimes |0\rangle\langle 0|^E + \frac{2}{3}|1\rangle\langle 1|^K \otimes |0\rangle\langle 0|^{E'}$

$= \left(\frac{1}{3}|0\rangle\langle 0| + \frac{2}{3}|1\rangle\langle 1|\right) \otimes |0\rangle\langle 0|^E$

⇒ Eve has some information about the key.

e.g. 4 Eve has a classical register also.

$\rho_{KE} = \sum_{k,e} P(k,e)\,|k\rangle\langle k| \otimes |e\rangle\langle e|$

$= \sum_k \left[\underbrace{P(k)}_{\frac{1}{|K|}} |k\rangle\langle k| \otimes \left(\sum_e \underbrace{P(e|k)}_{P(e)} |e\rangle\langle e| \right) \right]$

Condition of ignorance classical

§3.2 Trace distance & its use in security definitions

§3.2.1 operational interpretation

What does it mean to be almost ignorant

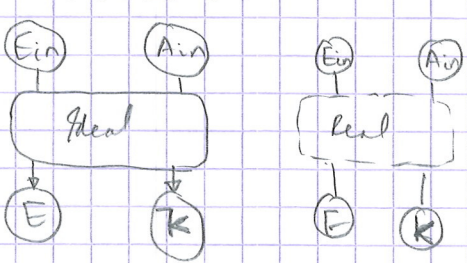
Perfection is impossible to attain in practice.

→ Errors are unavoidable in the real world

→ Any real protocol has finite amount of comm^n.

→ We will often perform tests - can only gain confidence

Real vs Ideal Scenario



The real protocol will never exactly produce ρ^{ideal}_{KE}

We will be happy if ρ^{real}_{KE} is "close enough" to ρ^{ideal}_{KE}

What does it mean to be "close"?

Distinguishing quantum states

$\rho^{ideal}_{KE} = \frac{1}{|K|} \otimes \rho_E$ with prob ½ → (KE)

ρ^{real}_{KE} with prob ½

Question. Which do we have? Real or ideal?

we make a measurement! M_{real} M_{ideal}

POVM: $M_{real} + M_{ideal} = \mathbb{1}$.

$P_{distinq} = \frac{1}{2}\mathrm{tr}\left(M_{ideal}\rho^{ideal}_{KE}\right) + \frac{1}{2}\mathrm{tr}\left(M_{real}\rho^{real}_{KE}\right)$

$= \frac{1}{2} + \frac{1}{2}\mathrm{tr}\left[M_{ideal}\left(\rho^{ideal}_{KE} - \rho^{real}_{KE}\right)\right]$

$0 \le M_{ideal} \le \mathbb{1}$ Positive Semidefinite

$\rho^{ideal}_{KE} = \frac{1}{|K|} \otimes \rho_E \leftrightarrow \rho^{real}_{KE}$ close

28 Oct 2016

Def^n trace distance := $D(\rho_1, \rho_2) = \max_{0 \le M \le 1} \mathrm{tr}(M(\rho_1 - \rho_2))$

Def^n; ϵ-close := $\rho_1 \approx_\epsilon \rho_2 \leftrightarrow D(\rho_1, \rho_2) \le \epsilon$

Why is the trace distance useful?

Larger protocol: e.g. one time pad might use this key.

Real → ρ_{KE}^{real} ↗ somewhat unknown but use the ideal state ∴ no measurement can really distinguish the states.

§ 3.2.2 Examples of the trace dist.

$\rho_0 = |0\rangle\langle 0|$ $\rho_1 = |1\rangle\langle 1|$

$M_0 = |0\rangle\langle 0|$ $M_1 = |1\rangle\langle 1|$

$p_{0|0} = tr[M_0\rho_0] = |\langle 0|0\rangle|^2 = 1 = p_{1|1}$

$p_{1|0} = tr[M_1\rho_0] = 0$

$p_{dist} = \frac{1}{2} tr[M_0\rho_0] + \frac{1}{2} tr[M_1\rho_1] = \frac{1}{2}\cdot 1 + \frac{1}{2}\cdot 1 = 1$

The trace distance: $D(\rho_0,\rho_1) = \max_M tr[M(\rho_0-\rho_1)]$

$= \max_{0\le M\le 1} tr[M(|0\rangle\langle 0| - |1\rangle\langle 1|)]$

≥ 0 ≥ 0

we want $tr M|1\rangle\langle 1|$ to be as small. Thus we can use $M = |0\rangle\langle 0|$ to get the max value.

$= 1 - 0 = 1$

§ 3.3 The (min)-entropy including the smooth min-entropy

§ 3.3.1 Quantify Randomness

Ideal case: uniformly random

$P(X=x) = \frac{1}{2^n}$ $\rho_X = \frac{\mathbb{1}}{2^n} = \left(\frac{\mathbb{1}_2}{2}\right)^{\otimes n}$

Randomness generat° box → $x = x_1,\dots,x_n \in \{0,1\}^n$

Attempt 1: Trace distance

Uniform except on one bit. $\rho_X = \left(\frac{\mathbb{1}_2}{2}\right)^{\otimes n-1} \otimes |0\rangle\langle 0|$

NB: But these two (see last lecture) can be distinguished quite well.

Attempt 2: "Entropy"

Def^n: $H(X) = -\sum_x P(x=x)\log P(x=x)$

e.g.: Ideal case, uniformly random $P(X=x) = \frac{1}{2^n}$, $H(X) = n$

e.g. 2: A box with $H(X) = \frac{n}{2}$; opening the box

$P(X=x) = \{\frac{1}{2}\ \ 11\cdots 1\}$ $\frac{1}{2}<\frac{1}{2^{n-1}}$ $\frac{1}{2^{n-1}}$ } other strings

(see rough for H)

Is it sensible to use this box instead of the n box? No: $\frac{1}{2}$ the times, the key can be guessed, regardless of n.

Answer: Min-entropy to the rescue

Def^n: $H_{min} := -\log \max_x P(X=x)$

Interp: − log of max. guessing prob. I will pick that key as a guess which has the highest probability of appearing, as an eavesdropper.

NB: In the worst case (for the box) $H_{min} = 1$

For the maximally mixed, $= n$

Properties

↳ Recall Neg. $D(\rho_1,\rho_2) \ge 0$

↳ 0 only when same $D(\rho_1,\rho_2) = 0 \Leftrightarrow \rho_1 = \rho_2$ [proof?]

↳ Symmetric $D(\rho_1,\rho_2) = D(\rho_2,\rho_1)$

↳ Triangle inequality $D(\rho_1,\rho_3) \le D(\rho_1,\rho_2) + D(\rho_2,\rho_3)$

[Doubt]: Prob of distinguishing always $> \frac{1}{2}$?

[Stupid]: Yeah, at random you can do $\frac{1}{2}$!

Example: one of many

$\rho_0 = |0\rangle\langle 0|^{\otimes n}$ $\rho_1 = |0\rangle\langle 0|^{\otimes n-1} \otimes |1\rangle\langle 1|$

$D(\rho_0,\rho_1) = \max_M tr[M(\rho_0-\rho_1)]$

$= \max_M tr[M|0\rangle\langle 0|^{\otimes n-1}(|0\rangle\langle 0| - |1\rangle\langle 1|)]$

$(|0\rangle\langle 0|)^{\otimes n-1} \otimes |0\rangle\langle 0|$

$= 1 - 0 = 1$

Example: Maximally mixed & $|0\rangle$

$\rho_0 = \frac{\mathbb{1}}{2}$ $\rho_1 = |0\rangle\langle 0|$

$D(\rho_0,\rho_1) = \max_M tr[M(\rho_0-\rho_1)]$

$= \max_M tr\left[M\left(\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| - |0\rangle\langle 0|\right)\right]$

$= \max_M \frac{1}{2} tr[M|1\rangle\langle 1|] - \frac{1}{2} tr[M|0\rangle\langle 0|]$

≥ 0 ≥ 0

$\Rightarrow M = |1\rangle\langle 1|$

$= \frac{1}{2}\cdot 1 = \frac{1}{2}$

§ 3.3.2 The conditional min entropy

Recall: For a classical string $H_{min}(X) = -\log \max_x P(X=x) = -\log P_{guess}(X)$

Consider: The eavesdropper has some information E about X.

∴ We have two systems, $\rho_{XE} = \sum_{x,e} P(X=x)P(E=e|X=x)|x\rangle\langle x| \otimes |e\rangle\langle e|$

X classical; E may be quantum. (has info about X)

Def^n: $H_{min}(X|E) = -\log \sum_e P(E=e) P_{guess}(X|E=e)$

Case: E is classical

Remark: Think of it as log of my prob. to guess granted I know E.

NB: $P_{guess}(X|E=e) = \max_x P(X=x|E=e)$

NB 2: But E could have quantum information

claim: A quantum side information is strictly more powerful than classical side information.

The min-entropy for c-q states

Case: E is quantum. $\rho_{XE} = \sum_x P(X=x)|x\rangle\langle x| \otimes \rho_x^E$

X — ρ_{XE} — E

31 Oct 2016

Recall: $H_{min}(X|E)_\rho = -\log P_{guess}(X|E)$

$P_{guess}(X|E) = \max \sum_x P(X=x)\, tr(M_x^E \rho_x^E)$

where $\sum_x M_x^E = \mathbb{I}_E$ & $\forall x, M_x^E \geq 0$ — measurement corresponding to x as a string.

— DOUBT: are M_x arbitrary? I thought they would have some well defined way of relating to x.

— clarified in the "blackboard"; see the git Hub folder.

Properties of the min-entropy of c-q states

(a) Largest & smallest values: $\log|X| \geq H_{min}(X|E)_\rho \geq 0$

proof: Recall $H_{min} = -\log P_{guess}$

Now worst case would have $P_{guess} = \frac{1}{|X|}$

Best case, $P_{guess} = 1$.

(b) Conditioning reduces entropy: $H_{min}(X|E)_\rho \geq H_{min}(X|EF)_\rho$

"proof": more knowledge can only incr. guessing prob.

(c) Reduction by one register: $H_{min}(X|EK)_\rho \geq H_{min}(X|K) - \log|E|$

$|E|$ = size of the register

What if the state is not known exactly?

$\rho_{XE} \approx_\epsilon \frac{1}{|X|} \otimes \rho_E$; what's the min entropy?

Remark/Claim: Min entropy is not as nice (smooth & continuous) as shannon entropy

Def^n: Smooth min-entropy := $H_{min}^\epsilon(X|E) = \max_{\tilde\rho_{XE} \in B^\epsilon(\rho_{XE})} H_{min}(X|E)_{\tilde\rho}$

Def^n: Epsilon Ball := $B^\epsilon(\rho_{XE}) := \{\tilde\rho_{XE} \mid D(\rho_{XE}, \tilde\rho_{XE}) \leq \epsilon\}$

E.g.: "Obviously" the $H_{min}^\epsilon(X|E)_{\rho_{XE}} = H_{min}(X|E)_{\frac{\mathbb{I}}{|X|}\otimes\rho_E}$

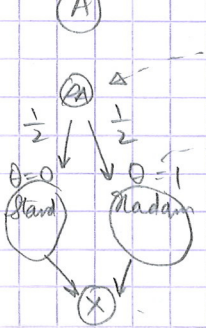
Doubt: Can't there be a "better" ρ_E' in the epsilon ball that yields a larger min entropy than say some other $\frac{\mathbb{I}}{|X|}\otimes\rho_E'$.

Ans: No because: this will have the highest value of H_{min} independent of ρ_E

§3.4 Uncertainty Principle: simple version BR84

§3.4.1 Uncertainty principle leads to security

Uncertainty game



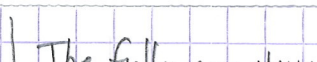
Claim: $\forall \rho_A, \frac{1}{2}\left[P_{guess}(X|\theta=0) + P_{guess}(X|\theta=1)\right] \leq c < 1$

For the Hadamard & the standard basis, $c = \frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.85$

proof: See rough

Remark: This shows uncertainty; if $P_{guess}(\theta=0)=1$, then $P_{guess}(\theta=1) < 1$.

The fully quantum min-entropy



Min entropy: $H_{min}(A|E) = -\log[|A| \, Dec(A|E)]$

Def^n: $Dec(A|E) = \max_{\Lambda_{E\to A'}} F(\Phi_{AA'}, \mathbb{I}_A \otimes \Lambda_{E\to A'}(\rho_{AE}))$

$\Phi_{AA'}$: max. entangled state.

Def: Fidelity: $F(\rho,\sigma) = tr(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}})$

NB: Fidelity = 1 for $\rho = \sigma$;

Claim: Fidelity gets smaller for states farther away.

Rationale: Classically we wanted to find that state x which was most correlated with the known register e.

Quantumly, we find the state E which is most close, viz. maximally entangled, with a state. (notionally equivalent of x).

§3.3.3 Example

$\rho_{XE} = \frac{1}{2}|0\rangle\langle 0| \otimes |0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| \otimes |+\rangle\langle +|$ (ρ_0^E, ρ_1^E)

Recall: $H_{min}(X|E) = -\log P_{guess}(X|E)$

$: P_{guess}(X|E) = \max_{\{M_x^E\}} \sum_x P(X=x)\, tr(M_x^E \rho_x^E)$

$P_{guess}(X|E) = \frac{1}{2} tr(M_0 \rho_0^E) + \frac{1}{2} tr(M_1 \rho_1^E)$

Recall: $M_0 + M_1 = \mathbb{I}$; $\Rightarrow = \frac{1}{2} tr(M_0 \rho_0^E) + \frac{1}{2} tr((\mathbb{I} - M_0)\rho_1^E)$

NB: $\rho_1 - \rho_2$ is hermitian $= \frac{1}{2} + \frac{1}{2} tr[M_0(\rho_0^E - \rho_1^E)]$

$\Rightarrow \rho_1 - \rho_2 = \sum_i \lambda_i |v_i\rangle\langle v_i|$ $= \frac{1}{2} + \frac{1}{2} D(\rho_0^E, \rho_1^E)$

NB 2: some λ_i are +ve, some are −ve. $= \frac{1}{2} + \frac{1}{2\sqrt{2}}$

$= \sum_{i \text{ for } \lambda_i > 0} |\lambda_i| |v_i\rangle\langle v_i| - \sum_{i \text{ for } \lambda_i < 0} |\lambda_i| |v_i\rangle\langle v_i|$

NB 3: since $tr\, M(|\lambda_i||v_i\rangle\langle v_i| - |\lambda_i||v_i\rangle\langle v_i|)$ would be highest if there's no neg. contribution "$\Rightarrow$" $M = \sum_{i(\lambda_i>0)} |v_i\rangle\langle v_i|$

calc: $\rho_0^E - \rho_1^E = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$

$= \begin{pmatrix} +\frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & -\frac{1}{2} \end{pmatrix}$

$= \frac{1}{\sqrt{2}}|\times| - \frac{1}{\sqrt{2}}|+\rangle\langle +|$

Claim: This holds even if Eve has an extra classical register

$\forall \rho_A \; \frac{1}{2}[P_{guess}(X|K\theta=0) + P_{guess}(X|K\theta=1)] \leq c < 1$

Recall: $H_{min} = -\log P_{guess}(X|K\theta)$

$= -\log c$

From a game to entropic uncertainty

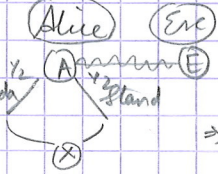
objective: Define this as a min entropy.

Extra inherent limitation in the guessing game:

$\forall \rho_A \; \frac{1}{2}(P_{guess}(X|\theta=0) + P_{guess}(X|\theta=1) \leq c < 1$

1 Nov 2016

What if Eve is Entangled with $A B_0$



for $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

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

$\Rightarrow$ Eve can guess with certainty

Uncertainty & Entanglement

No entanglement: Large uncertainty

$H_{min}(X|\theta E) \approx 0.22$

$+\log_2(0.85..))$

Maximal entanglement: $H_{min}(X|\theta E) = 0$

(Some entanglement: Some uncertainty

Claim: $H^E_{min}(X|\theta E) \geq f_M(H_{min}(A|E))$

§ 3.5 Extended UR principles: tripartite version

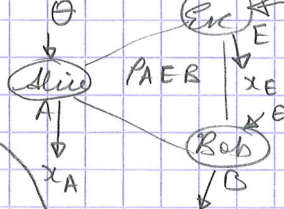
§ 3.5.1 Uncertainty and monogamy of entanglement

Remark: Eve is uncertain when there's little entanglement. How to ensure little entanglement?

Recall: Bell tests can be used to test for entanglement.

NB: Can't ask Eve to do a bell test; we don't trust her, don't know if she exists or may not even be present

Sol^n: Look at three parties instead of 2.



Game: (i) Alice performs a measurement in the Hadamard or standard basis (θ)

(ii) Eve must guess Alice's outcome, given θ.

(iii) same for Bob.

win: When both Bob & Eve guess the outcome correctly. $x_A = x_B$ & $x_A = x_E$.

Ans: $p_{win} = \frac{1}{2}\sum_\theta \sum_x P(X_A = x, X_B = x, X_C = x \,|\, \Theta = \theta)$

{ long calc (see official lecture notes)

$\max_{\substack{P_{ABE} \\ M^E, M^B}} p_{win} = \frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.85$

Insight:

1) If Eve & Alice are highly entangled with each other, then Eve will have no uncertainty.

2) Recall: Entanglement is monogamous.

$\Rightarrow$: There must be very little entanglement b/w Alice & Bob.

$\Rightarrow$: If Alice & Bob are entangled, Eve is highly uncertain about Alice

3) How to test for entanglement b/w Alice & Bob (a) Bell test

(b) By preparing the state s.t. Bob always wins.

e.g. $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)$

$\therefore$ If Alice & Bob almost always yield $x_A = x_B$ it must mean that $x_C = x_A = x_B$ must have errors $\therefore$ the pr winning is bounded.

Recall: This is the same as for a 2 player game.

Teaser: This can be used to prove security of Quantum Protocols

Next Target: Write these as entropy & find the highest prob. of Eve guessing either Alice's or Bob's outcome.

Teaser: H_{min}

§ 3.4.2 Example: Hadamard & standard basis

Objective: Calculate $H_{min}(X|\Theta) = -\log P_{guess}(X|\Theta)$ for this system

$P_{guess}(X|\Theta) = \frac{1}{2} P_{guess}(X|\Theta=0) + \frac{1}{2} P_{guess}(X|\Theta=1)$

The guessing prob. is obviously given by

$P_{guess}(X|\Theta=0) = \max_{x_0} P(X = x_0 \,|\, \Theta = 0)$

$= \max_{x_0} tr(\rho_A |x_0\rangle\langle x_0|)$

$P_{guess}(X|\Theta=1) = \max_{x_1} P(X = x_1 \,|\, \Theta = 1)$

$= \max_{x_1} tr(\rho_A |x_1\rangle\langle x_1|)$

where $|x_0\rangle \in \{|0\rangle, |1\rangle\}$

$|x_1\rangle \in \{|+\rangle, |-\rangle\}$

Effectively then

$P_{guess} = \frac{1}{2}\{tr[\rho_A |x_0\rangle\langle x_0|] + tr[\rho_A |x_1\rangle\langle x_1|]\}$

$= \frac{1}{2}\{tr[\rho_A (|x_0\rangle\langle x_0| + |x_1\rangle\langle x_1|)]\}$

NB: This corresponds to finding the largest eigenvalue of this matrix & choose x_0, x_1 to find the matrix that yields the largest among the largest eigenvalues, $\therefore$ Eve can always choose ρ_A to give at most this # that will maximizes her guessing prob.

NB: See the rough, you have done this independently

Standard vs Hadamard

Ques: What is the winning probability?

---

§ 3.5.2 Example: Intuition

$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$

$\rho_{ABE} = |\psi\rangle\langle\psi|_{AB} \otimes |0\rangle\langle 0|_E$

Comment: Example where Alice & Bob share an entangled state. We assume (to get intuition) that Alice & Bob both measure in Hadamard or standard basis depending on θ.

$\Rightarrow$ $x_A = x_B$ always. We now need to find prob of $x_A = x_B$.

$$\rho_{AE} = \frac{\mathbb{1}_A}{2} \otimes |0\rangle\langle 0|_E$$

$x_A = x_A$ happens with prob $1/2$

NB: Prob. Alice ends on a mixed state, an output x_A, $P(x_A = x_A) = \mathrm{tr}\left(\frac{\mathbb{1}}{2} |x_A\rangle\langle x_A|\right) = \frac{1}{2}$

$$P_{guess}(X|E,\Theta=0) = \frac{1}{2} \max_{M^E} \sum_{\substack{x_A \\ = x_E}} \mathrm{tr}\left[M^E_{x_E} |0\rangle\langle 0|_E\right]$$

NB: $M^E_0 + M^E_1 = \mathbb{1}$

$$= \frac{1}{2} \mathrm{tr}\left[\mathbb{1} |0\rangle\langle 0|_E\right] = \frac{1}{2}$$