Week #4
FROM IMPERFECT INFORMATION TO (NEAR) PERFECT SECURITY

§ 4.1 Privacy Amplification

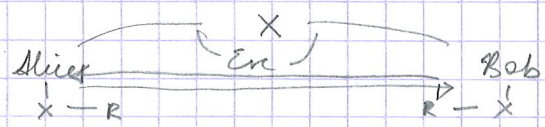
§ 4.1.1

Remark: Usually the last step in key distⁿ protocols
: Reduces the objective of producing keys which are (a) uniformly random & (b) uncorrelated with the Eve's dropper,
↓
some amount of uncertainty

Lit: First done by Bennett & Brassard (cf BB84) & Robert "Privacy Amplification by Public Discussion"

Idea: "... assume that Alice & Bob wish to agree on a secret random bit string and have at their disposal an imperfect private channel & a perfect public channel..."

Amplifying a weak secret



Imagine: string $X \in \{0,1\}^n$; may or may not be uniformly distr
: Eve could keep some side info
eg. $\{ x_1, x_1 x_3 x_5 \cdots$ parity ρ_X^E

Objective: Use private & public channel to arrive at a string $R \in \{0,1\}^m$ with $m \leq n$ s.t. R is uniformly distributed i.e. $R \sim U_m$ & $\rho_{RE} \sim 2^{-m} \mathbb{1}_R \otimes \rho_E$ i.e. uncorrelated.

Privacy Amplification

ρ_{XE} (classical / quantum; c/Q)

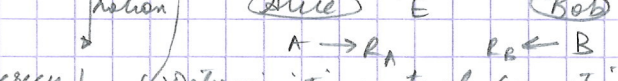
Aim: Design a protocol s.t.
$P_r(R_A \neq R_B) \leq \varepsilon_c$ (correctness)
$\| \rho_{R_A E} - 2^{-m} \mathbb{1}_{R_A} \otimes \rho_E \|_{tr} \leq \varepsilon_s$ (secrecy)

NB: The side information should be allowed to contain the public communication, K. (proper notion)

$\Rightarrow \| \rho_{R_A K E} - 2^{-m} \mathbb{1}_{R_A} \otimes \rho_{KE} \|_{tr} \leq \varepsilon_s$ (secrecy)

Also we'll start with assuming $H_{min}(X|E) \geq k$ for our private communication protocol

Q: Do we really need to communicate? (i.e. that info gets leaked to Eve & she can use that to crack)
claim: Yes.
"Proof": Argue by assuming no communicⁿ



(a) Deterministic protocol (an option)
$R = f(X)$ for some fixed f.
claim: breakable; ∵ f is known (protocols are known), then even if Eve keeps $f(x)$, , security is lost.
(b) We need Randomness; trouble: $R_A \neq R_B$ in general.
(c) Synchronize (interaction) to ensure $R_A = R_B$.

§ 4.1.2 Amplifying a weak secret

Simplified case: X : uniform n bits $\in \{0,1\}^n$
(assume) E : pn bits of X (Eve has access to these)
for $0 < p < 1$

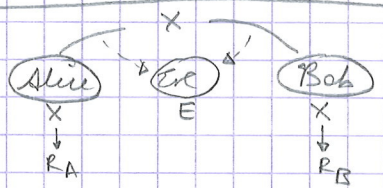


Illustration: $X_1 X_2 \cdots X_{n-1} X_n$
$\perp$ $X_2 \cdots \perp \perp X_n$

e.g. use the parity $R = X_1 \oplus \cdots \oplus X_n$
∵ so long as even one bit is not known to the Eve's dropper, the parity will remain random for him. (of course for $p \neq 1$)
claim: Very hard to extract more;
: We need randomness to extract more than 2 bits.

start: 7 Nov 2016

e.g. 2: Alice constructs $Y_1 \cdots Y_m \in \{0,1\}^n$ randomly & sends them to Bob.
$R = X \cdot Y_1, X \cdot Y_2, \ldots X \cdot Y_m \in \{0,1\}^m$
NB: Even if Eve knows $Y_1 \cdots Y_m$, she can't find R without knowing X completely.
claim: R is uniformly random.
"proof": $Pr(X \cdot Y_m = 0 \mid X \sim U_n, X \cdot Y_1 = a_1, \ldots, X \cdot Y_{m-1} = a_{m-1}, X \cdot e_1 = b_1, \ldots X \cdot e_{np} = b_{np})$
Df^n: U_n := uniformly random in n bits.

where e_1 in this ex is $(0\,1\,0\ldots)$ i.e. $X \cdot e_1 = X_2 = a_1$ & so on.
$\{e\}$ capture which bit Eve has.

Here we have $m-1+np$ linear eq^{n}s which specify $2^{n-(m-1+np)}$ dimensional (# of elements(i)) subspace of $\{0,1\}^n$. In this subspace also X should be uniformly random. Now so long as Y_m is linearly independent of the remaining $Y_{m'}$s, $X \cdot Y_m$ will also be random

claim: ϵ_s secure; $\epsilon_s \sim \left(\frac{1}{2}\right)^{n-m-1+np}$ ($\because$ larger the subspace, better the security)

$m \lesssim (1-p)n$

Intuition: consistent $\because$ there're $(1-p)n$ bits which the Eavesdropper doesn't know, so that's the max # of bits we should be able to extract (free bits).

End: 7 Nov 2016

§ 4.2 What's an extractor and why does it achieve that task?

§ 4.2.1

Motivation: Randomness Extractors: objects with the goal to map random variables with enough entropy, to random variables as close to being uniformly distr as possible

From partial to uniform randomness

$H_{min}(X|E)_\rho \geq k$ (all we know)

$\xrightarrow{Ext}$ $Z \in \{0,1\}^m = Ext(X,Y)$ (extra randomness)

$\rho_{ZEY} \approx U_m \otimes \rho_{EY}$

$Y \in_R \{0,1\}^d$ (random)

$2^{-m}\mathbb{1}$

Strong Extractors: Y is included in the ext

$\rho_{ZEY} \approx U_m \otimes \rho_{EY}$

Weak Extractors: $\rho_{ZE} \approx U_m \otimes \rho_E$

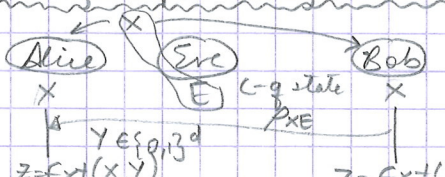
goals: maximize m: $m \approx k$ (think as $\lesssim (1-p)n$, $0<p<1$)

small d (for best efficiency):

(claim): $d \gtrsim \log(n/\epsilon)$

(eg. $\epsilon \approx 2^{-0.1n} \rightarrow d \gtrsim 0.1n$)

Privacy Amplif^n using seeded extractors



objective: use an extractor to amplify

assume: Alice has a random # generator that's independent of Eve & X.

correct $\epsilon_c = 0$

security $\| \rho_{R_A E Y} - \frac{1}{|R_A|}\mathbb{1}_{R_A} \otimes \rho_{EY} \|_c \leq \epsilon_s$ (same as the security of the extractor)

Strong seeded Extractors

Def^n: $Ext: \underbrace{\{0,1\}^n}_{X} \times \underbrace{\{0,1\}^d}_{Y} \rightarrow \underbrace{\{0,1\}^m}_{Z}$

"source" "seed" "output"

is a (k,ϵ) strong extractor if $H_{min}(X|E) \geq k$

$\| \rho_{Ext(X,Y)YE} - \mathbb{1} \otimes \rho_{YE} \|_{tr} \leq \epsilon$

where

n: input/source length

d: seed length

m: output length.

k: input/source entropy

ϵ: Error

§ 4.2.2 Example: A strong extractor against bit fixing sources

A strong extractor

X: n bits

E: pn bits of X $\Rightarrow H_{min}(X|E) = (1-p)n$

$Y = (Y_1, \ldots, Y_m)$: nm' uniform bits

($Y_1, \ldots, Y_m$ each $\in \{0,1\}^n$; $d = nm'$)

goal: Extract as many of such bits as possible.

Recall: $Ext: \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m$ is (k,ϵ) they for $H_{min}(X|E) \geq k \Rightarrow \| \rho_{Ext(X,Y)YE} - \frac{1}{|Z|}\mathbb{1} \otimes \rho_{YE} \|_{tr} \leq \epsilon$

claim: $Ext(X,Y) = (X \cdot Y_1, \ldots, X \cdot Y_m) \in \{0,1\}^m$

aim: show this is uniformly distributed conditioned on both the side information & the seed Y.

idea: Think of this procedure as a matrix mult. over the binary field.

$A = [Y_1 \; Y_2 \; \cdots \; Y_m]$ $\quad X = [\;\; \leftarrow \text{fixed}]$

$Z = AX$

Commentary: Some bits in X are fixed. 0 or 1 $\Rightarrow$ some columns are either taken or they're not.

: The other coordinates get chosen a random depending on X.

$\dim\left[\text{span}\{\text{non-fixed columns}\}\right] \geq m$

Then the output will be uniformly distributed.

$(1-p)n \geq m$ (much larger)

Then secure (TODO: careful proof)

Drawback: The seed is quite large; it grows as n^2 ($m \sim n^2$)

§ 4.3 Randomness extraction using two-universal hashing

§ 4.3.1 An extractor construction based on two-universal hash functions

Recall: strong seeded extractors $\xrightarrow{\text{privacy amplif}^n}$

idea: connection b/w hash f^n's & extractors.

A combinatorial view of extractors

assume: no side-info (simplicity)

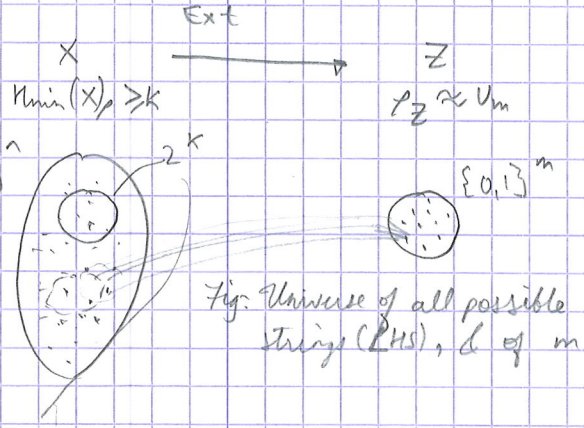


Fig: Universe of all possible n bit strings (LHS), & of m bit (up).

claim: To first approx., X is uniformly distr on a subset of the universe of size K.

NB: Larger the K, more uncertain

procedure: A map from big set to small set ensuring it's distributed once a large enough subset.

7 NOV 2016

NB2: We can't use deterministic assignment. Else multiple points may map to the same point (as shown) & if my string X is on that set of points, then my output is known thus not secure.

NB3: Using a random seed might help. choose a map depending on the seed, granted we have chosen the source already.

1- Universal Hash f^ns

Def^n: Hash f^n := maps $\mathcal{H}: \{f_y: \{0,1\}^n \to \{0,1\}^m\}$

Def^n: 1-Universal := $\Pr_y[f_y(x) = z] = 2^{-m}$ $\forall x, z$

e.g. $y \in \{0,1\}^n$
$f_y(x) = x \oplus y$
is 1-universal.

NB: Not secure! If X is not uniform, say has x_1 fixed, then from z & y I can learn x_1. Consequently x is not uniformly random for me.

Def^n: 2-Universal := $\Pr_y[f_y(x) = z \ \& \ f_y(x') = z'] = 2^{-2m}$ $\forall x \neq x'$, $z = z'$

e.g. $f_y(x) = x \oplus y$ is not 2-universal;

proof: $\Pr(x \oplus y = z \ \& \ x' \oplus y = z')$
$\stackrel{?}{=} \Pr(x \oplus y = z \ \& \ x \oplus x' = z \oplus z') = 0$ when $x \neq x', z = z'$

e.g. $f_y(x) = x \cdot y \in \{0,1\}$ $(m=1)$
my 'proof': $\Pr(x \cdot y = z \ \& \ x' \cdot y = z')$
$= \Pr(x \cdot y = z \ \& \ (x-x') \cdot y = z' - z)$
at least doesn't have the same problem as above.

From 2-universal hashing to extractors

CASE: no side info

Setup:
X (source), $H_{min}(X) \geq K$
Ext, $y \sim U_d$
$Z = f_y(X)$
$\rho_{ZY} \approx U_m \otimes U_d$

argument: fixing a y, $z, z' \in \{\{0,0\},\{0,1\},\{1,0\}$ & $\{x \cdot y, x' \cdot y\}$ have these values $\{1,1\}\}$ with equal probability, once y is averaged over.

NB: Without the average, say x_1 was fixed, then $y = (1,0,0,\ldots)$ would (high prob) yield a contradiction.

1) Collision probability: $CP(\{P_i\}) = \sum P_i^2$

Def^n: Collision probability := sum of squares of the prob. distribution.

Intuition: Lower the CP, closer to uniform

2) From collision probability to trace dist (statistical dist. here)

idea: Show this trace dist is a f^n of CP.

Let's start with (1)

$CP(Y,Z) = \sum_{y,z} \Pr(Y=y, Z=z)^2 = \sum_{y,z} \Pr(Y=y)^2 \Pr(Z=z \mid Y=y)^2$

$= \sum_{y,z} 2^{-2d} \left(\sum_x P_x(x) 1_{f_y(x)=z}\right)^2$

$= \sum_{y,z} 2^{-2d} \left(\sum_{x,x'} P_{x_1}(x) P_{x_1}(x') \underbrace{1_{f_y(x)=z=f_y(x')}}_{\text{for } x \neq x'}\right)$

$P_{x_1}(\cdot) = 2^{-2m}$ for $x = x'$ (the statement always holds)

from the prop of 2 universal hash f^n

We get two terms then & using the fact that the min entr is at least K

$\leq 2^{-d}\left(\underbrace{2^{-k}}_{x=x' \text{ terms}} + \underbrace{2^{-m}}_{\text{bounded by this granted due Lax summed over } z}\right)$

Left over Hash Lemma!!

Now we try (2), bounding the statistical distance.

$\sum_{yz} \left|\Pr(Y=y, Z=z) - 2^{-d}2^{-m}\right|$

$\leq 2^{\frac{d+m}{2}} \left(CP(Y,Z) - 2^{-(d+m)}\right)^{1/2}$ (claim)

(use Cauchy Schwarz for random variables)

Now substitute for CP's bound to get

$\leq 2^{\frac{d+m}{2}} 2^{-\frac{d+k}{2}} = 2^{\frac{m-k}{2}} = \epsilon$

Result: As long as $m << k$, $\to \epsilon$ that's very small.

If $\mathcal{H}$ is a 2-universal family of hash f^ns $f: \{0,1\}^n \to \{0,1\}^m$ Then $Ext(x,y) = f_y(x)$ is a (K, ϵ) strong extractor for any $K \geq m + 2\log\frac{1}{\epsilon}$

§4.3.2 A family of 2-universal hash functions

Recall: $\{f_i: \{0,1\}^n \to \{0,1\}^m\}$
: 2-universal: $\Pr_i[f_i(x) = z \ \& \ f_i(x') = z'] = 2^{-2m}$

Remark: Use a field instead $\mathcal{H}: \{f: \mathbb{F} \to \mathbb{F}\}$ where $\mathbb{F}$ is a finite field, e.g. $\mathbb{F}_{2^n}$ (just truncate)

e.g. $H = \{f_{a,b}: \mathbb{F} \to \mathbb{F} \quad a,b \in \mathbb{F}\}$
all affine f^ns $x \longmapsto ax + b$

Remark: (1) Easy to evaluate; (2) $|H| = |\mathbb{F}|^2 = 2^{2n}$ size of seed; size of i/p

NB: that's linear in the length of input.

Check: 2-Universal?

$x \neq x'$, $z = z'$

$$\Pr_{a,b}\begin{bmatrix} ax+b=z \\ ax'+b=z' \end{bmatrix} = \Pr_{a,b}\begin{bmatrix} b=z-ax \\ a(x'-x)=z'-z \end{bmatrix} = \Pr_{a,b}\left[a(x'-x)=z'-z\right].$$

$$\Pr\left[b=z-ax \,\middle|\, a(x'-x)=z-z'\right]$$

$$= \Pr_{a,b}\left[a=(z'-z)/(x'-x)\right] \cdot \Pr\left[b=z-ax \,\middle|\, a(x'-x)=z-z'\right] = |\mathbb{F}|^{-2} = 2^{-2m}$$

$\because m=n$ in this case.

- $\Pr_{a,b}[a=(z'-z)/(x'-x)] = |\mathbb{F}|^{-1}$: uniformly random; non-zero fixed element
- $\Pr[b=z-ax \mid a(x'-x)=z-z'] = |\mathbb{F}|^{-1}$: uniform random fixed; fixed here

Comment: This holds even when there is quantum side information.

§4.4 The Pretty Good Measurement

§4.4.1 Distinguishing Quantum States

Intuitive Objective := given $\{\rho_x^E\}$ what is the best guessing measurement $\rho_x^E \to x$?

Formal goal := $\max_{\{\Pi_x\}} \sum_x \mathrm{tr}(\Pi_x \rho_x^E)$ over all POVMs on E with $\Pi_x \geq 0$ & $\sum_x \Pi_x = \mathbb{I}_E$

Recall: $p_{\text{guess}}(X|E) := 2^{-H_{\min}(X|E)}$

NB: The goal is not to compute this number, but to find the measurement.

Remark: This problem is hard in general.

Case: $|x|=2$: the Helstrom measurement

$$\max\left[\mathrm{tr}(\Pi_0\rho_0) + \mathrm{tr}(\Pi_1\rho_1)\right]$$

$$= \max\left[\frac{1}{2}\mathrm{tr}\left[(\Pi_0+\Pi_1)(\rho_0+\rho_1)\right] + \frac{1}{2}\mathrm{tr}\left((\Pi_0-\Pi_1)(\rho_0-\rho_1)\right)\right]$$

$$= \frac{1}{2} + \frac{1}{2}\max_{-\mathbb{I}\leq\Pi\leq\mathbb{I}} \mathrm{tr}\left((\Pi_0-\Pi_1)(\rho_0-\rho_1)\right)$$

$$\leq \frac{1}{2} + \frac{1}{2}\|\rho_0-\rho_1\|_{tr}$$

where this is achieved by $\Pi_0 = (\rho_0-\rho_1)_+$ (positive eigenspace), $\Pi_1 = (\rho_0-\rho_1)_-$ (negative eigenspace)

§4.4.2 The PGM in Action

$x \in \{0,1\}^2$ $\rho_{00} = \frac{1}{4}|0\rangle\langle 0|$, $\rho_{01} = \frac{1}{4}|1\rangle\langle 1|$, $\rho_{10} = \frac{1}{4}|+\rangle\langle +|$, $\rho_{11} = \frac{1}{4}|-\rangle\langle -|$

$\rho = \sum_x \rho_x = \frac{1}{4}\mathbb{I} + \frac{1}{4}\mathbb{I} = \frac{1}{2}\mathbb{I}$ check: $\mathrm{tr}(\rho)=1$ ✓

$M_x = \rho^{-1/2}\rho_x\rho^{-1/2}$; $\rho^{-1/2} = \sqrt{2}\,\mathbb{I}$

$\Rightarrow M_{00} = \frac{1}{2}|0\rangle\langle 0|$, $M_{10} = \frac{1}{2}|+\rangle\langle +|$

$M_{11} = \frac{1}{2}|1\rangle\langle 1|$, $M_{01} = \frac{1}{2}|-\rangle\langle -|$

$$p_{\text{guess}}(\text{PGM}) = \sum_x \mathrm{tr}(M_x\rho_x) = 4\cdot\frac{1}{8} = \frac{1}{2}$$

$\Rightarrow H_{\min}(X|E)_\rho \geq \frac{1}{2}\left(-\log\frac{1}{2}\right) \geq 1/2$

claim: $H_{\min}(X|E) = 1$

§4.5 Extractor and Actual Privacy Amplific^n

8 NOV 2016

§4.5.1

Comment: Put everything together

Recall:

$\mathcal{H}: \{f_y: \{0,1\}^n \to \{0,1\}^m\}$

2-universal: $\Pr_y[f_y(x)=z \;\&\; f_y(x')=z'] = 2^{-2m}$

X —Ext→ $Z = f_y(X)$, with $Y \sim U_d$

$H_{\min}(X)_\rho \geq k$

$\rho_{ZY} \approx U_m \otimes U_d$ ← use 2-universal hash as an extractor; requirement "strong"

Case: $|x|>2$: The pretty good measurement (PGM)

Comment: Let's start with the classical case.

$\rho_x^E = p_x \in [0,1]$ opt: guess "x_0" s.t. $p_{x_0} = \max_x p_x$

Def^n: PGM: guess "x" according to the probability distribution p_x itself.

: choose $\Pi_x = p_x$

$$p_{\text{guess}}(\text{PGM}) = \sum_x \mathrm{tr}(\Pi_x\rho_x^E) = \sum_x p_x^2 \geq \max_x p_x^2 = p_{\text{guess}}^2$$

Remark: So the new PGM's prob of guessing is lower bounded by the square of the optimal guessing prob. (not too bad); $p_{\text{guess}}^2 \leq p_{\text{PGM}} \leq p_{\text{guess}}$

NB: Take $-\log$ & you'll get $H_{\min}(X|E) \geq -\frac{1}{2}\log[p_{\text{guess}}(\text{PGM})]$

Quantum case: (PGM)

ρ_x^E; try: $M_x \overset{?}{=} \rho_x^E$ no, don't $\sum M_x \neq \mathbb{I}$

claim: $M_x = (\rho^E)^{-1/2}\rho_x^E(\rho^E)^{-1/2}$

check: $\sum_x M_x = (\rho^E)^{-1/2}\rho^E(\rho^E)^{-1/2} = (\rho^E)^2 = \mathbb{I}$

where we used $\rho^E = \sum_x \rho_x^E$.

: $M_x \geq 0$ ∵ conjugated by a the op

$$p_{\text{guess}} = \sum_x \mathrm{tr}(OPT_x\rho_x^E)$$

$$= \sum_x \mathrm{tr}\left(\rho^{1/4}OPT_x\rho^{-1/4}\rho_x^{1/4}\rho_x\rho_x^{1/4}\rho^{-1/4}\right)$$ ← any set of POVMs that achieve the best possible guess.

Cauchy-Schwarz inequality

$$\leq \left(\sum_x \mathrm{tr}\left(\rho^{1/4}OPT_x\rho^{1/2}OPT_x\rho^{1/4}\right)\right)^{1/2}\left(\sum_x \mathrm{tr}\left(\rho^{-1/4}\rho_x\rho^{-1/2}\rho_x\rho^{-1/4}\right)\right)^{1/2}$$

($\sum_x OPT_x \leq \mathbb{I}$)

$$\leq \left(\sum_x \mathrm{tr}(OPT_x\rho)\right)^{1/2}\left(\sum_x \mathrm{tr}(M_x\rho_x)\right)^{1/2}$$

($\because \sum_x OPT_x = \mathbb{I}$)

$$\leq 1 \cdot \sqrt{p_{\text{succ}}(\text{PGM})}$$

applying $\log$, we again get $H_{\min}(X|E) \geq -\frac{1}{2}\log(p_{\text{guess}}(\text{PGM}))$

Remark: This is useful because it PGMs have a form independent of the form of ρ_x.

The optimal measurement can be very hard to find.

This doesn't do too bad.

When no side information:
"left-over hash lemma": If $\mathcal{H}$ is a 2-universal family then
$\mathrm{Ext}(X,Y) = f_Y(X)$ is a (K,ϵ) strong extractor
for any $K \geq m + 2\log(1/\epsilon)$

§4.5.2 The Universal Extractor in action

Comment: We'll apply our 2-universal hashing protocol to a simple example.

Now: 2 Universal-hashing extractor: Quantum Proof

$$\begin{array}{ccc} X & \xrightarrow{\mathrm{Ext}} & Z = f_Y(X) \\ & \uparrow & \\ H_{\min}(X|E)_\rho \geq K & Y \sim U_d & \rho_{ZYE} \approx U_m \otimes U_d \otimes \rho_E \end{array}$$

Goal: $2^{-d} \sum_{z,y} \| \rho^{E}_{zy} - \rho^{E} \|_{tr} < \epsilon$ for any $\{\rho^E_x\}$

s.t. $H_{\min}(X|E)_\rho \geq K$, where

Def^n: $\rho^E_{zy} := \sum_{x:\, f_y(x)=z} \rho^E_x$

Def^n: ρ^E_x (mixed) $:= \rho^E = 2^{-d} \sum_y \rho^E_{zy}$

NB: Substituting for ρ^E in the trace dist^n is this

1) From trace distance to collision prob.

Claim: $D(\rho_{ZYE}, 2^{-m} \mathbb{1} \otimes 2^{-d} \mathbb{1} \otimes \rho_E) \leq 2^{\frac{m}{2}-1} \left(2^d \sum_{z,y} \mathrm{tr}\left(\rho^E_{zy} \rho^{-\gamma_2} \rho^E_{zy} \rho^{-\gamma_2} \right) - 2^{-d} \right)^{1/4}$

$\mathrm{Ext}(X,Y)$ — $CP(ZY)$

2) Bounding the collision prob via the PA M

$CP(ZY) \leq 2^{-(d+m)} + 2^{-(d+K)}$;

$\epsilon = D(\ldots) \leq 2^{\frac{m}{2}-1} \cdot 2^{-\frac{K}{2}}$

Lemma: A strong quantum-proof extractor

$$\begin{array}{ccc} X & \xrightarrow{\mathrm{Ext}} & Z = f_Y(X) \\ & \uparrow & \\ H_{\min}(X|E)_\rho \geq K & Y \sim U_d & \rho_{XYE} \approx U_m \otimes U_d \otimes \rho_E \end{array}$$

"Quantum-proof left over hash lemma":
If $\mathcal{H}$ is a 2-universal family then $\mathrm{Ext}(X,Y) = f_Y(X)$ is a (K,ϵ) strong quantum-proof extractor for any $K \geq m + 2\log(1/\epsilon)$.

The two-universal-hashing extractor in action

$\rho_1 = \frac{1}{5}|0\rangle\langle 0|$, $\rho_2 = \frac{1}{5}|1\rangle\langle 1|$, $\rho_3 = \frac{1}{10}\mathbb{1}$, $\rho_4 = \frac{1}{5}|+\rangle\langle +|$

$\rho_5 = \frac{1}{5}|-\rangle\langle -|$; ← side information

$X \in \{1,2,3,4,5\} \in \mathbb{F}_5$ $\quad \mathcal{H} = \left\{ f_{ab} : \begin{array}{l} x \mapsto ax+b \\ a,b \in \mathbb{F}_5 \end{array} \right\}$

$\mathrm{Ext}(x,(a,b)) = f_{a,b}(x)$ $\quad m \leq \frac{K}{2} - \log(1/\epsilon)$

NB: The output m must satisfy →

For the time being, we simply use $(f_{a,b}(x) \bmod 2)$

e.g. $(a,b) = (2,3)$

x	$f_{a,b}(x)$	Ext
1	0	0
2	2	0
3	4	0
4	1	1
5	3	1

$\rho^E_{Z=0,Y=(2,3)} = \frac{1}{5}|0\rangle\langle 0| + \frac{1}{5}|1\rangle\langle 1| + \frac{1}{10}\mathbb{1} = \frac{3}{10}\mathbb{1}$

$\rho^E_{Z=1,y=(2,3)} = \frac{1}{5}|+\rangle\langle +| + \frac{1}{5}|-\rangle\langle -| = \frac{2}{10}\mathbb{1}$

NB: $\frac{3}{10}$ & $\frac{2}{10}$ are artefacts of smallness of the example.

NB2: The hashing mixes the side information s.t. both are $\propto \mathbb{1}$ & independent of Z (roughly)