10.1 (Computationally unbounded adversaries). Show that an anonymous key exchange protocol P (as in Definition 10.1) cannot be secure against a computationally unbounded adversary. This explains why all protocols in this chapter must rely on computational assumptions.

for computationally unbounded adversaries, doing key exhaustive search would take less than exponential time.
but $O(n)$ instead, thus $\text{Anon-K-Eadv}[\mathcal{A}, P]$ is non-negligible.

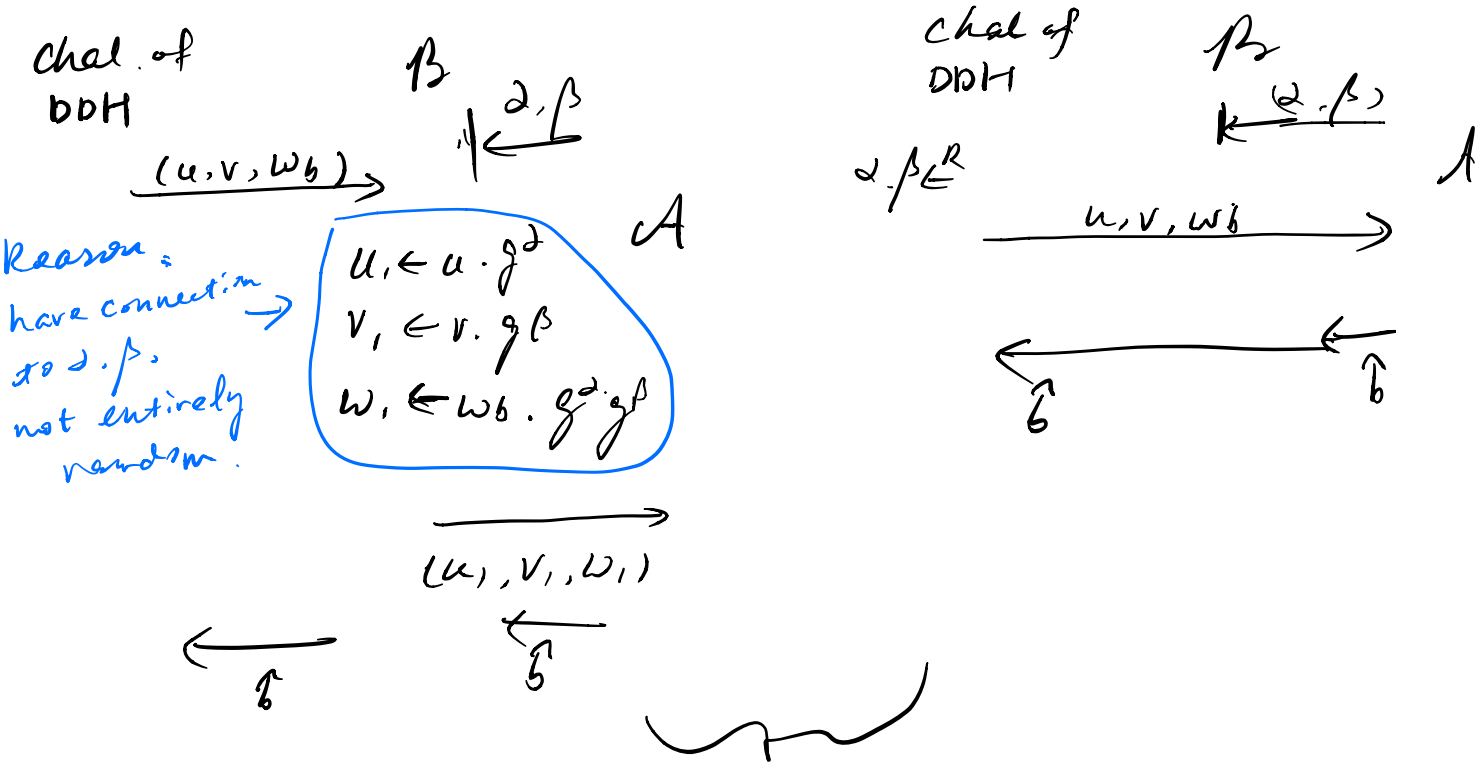
10.2 (DDH PRG). Let $\mathbb{G}$ be a cyclic group of prime order q generated by $g \in \mathbb{G}$. Consider the following PRG defined over $(\mathbb{Z}_q^2,\ \mathbb{G}^3)$:

$$G(\alpha, \beta) := (g^\alpha, g^\beta, g^{\alpha\beta}).$$

Show that G is a secure PRG assuming DDH holds in $\mathbb{G}$.

DDH: g^λ ($\lambda = \alpha\cdot\beta$) is indistn. from random $d \in \mathbb{G}$..

DDH adv $\longrightarrow$ PRG adv.



IMO, B with $\mathcal{B}$ are efficient & works as proof of

$\text{DDH-adv}[\mathcal{B}, \mathbb{G}] = \text{PRG-adv}[\mathcal{A}, G]$

10.3 (The Naor-Reingold PRF). Let $\mathbb{G}$ be a cyclic group of prime order q generated by $g \in \mathbb{G}$. Let us show that the following PRF defined over $\left(\mathbb{Z}_q^{n+1},\ \{0,1\}^n,\ \mathbb{G}\right)$ is secure assuming DDH holds in $\mathbb{G}$:

$$F_{\mathrm{NR}}\Big(\ (\alpha_0, \alpha_1, \ldots, \alpha_n),\ (x_1, \ldots, x_n)\ \Big) := g^{\left(\alpha_0 \cdot \alpha_1^{x_1} \cdots \alpha_n^{x_n}\right)}$$

This secure PRF is called the Naor-Reingold PRF. ↳ input x of n bit in size.

(a) We prove security of F_{NR} using Exercise 4.18. First, show that F_{NR} is an *augmented tree construction* constructed from the PRG: $G_{\mathrm{NR}}(\alpha, g^\beta) := (g^\beta, g^{\alpha\beta})$.

(b) Second, show that G_{NR} satisfies the hypothesis of Exercise 4.18 part (b), assuming DDH holds in $\mathbb{G}$. Use the result of Exercise 10.10.

Security of F_{NR} now follows from Exercise 4.18 part (b).

Discussion: See Exercise 11.1 for a simpler PRF from the DDH assumption, but in the random oracle model.

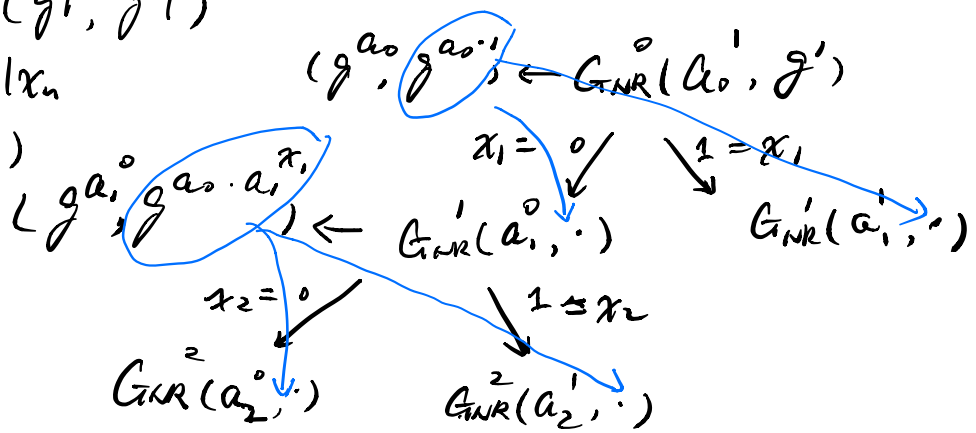
(a) $G_{NR}(\alpha, g^\beta) := (g^\beta, g^{\alpha\beta})$

for $x = x_1 \| x_2 \| \cdots \| x_n$

$(g^{\alpha_n^{x_n}}, y_n) \leftarrow G_{NR}^n(\alpha_n^{x_n}, y_{n-1})$

$F_{NR} \leftarrow y_n$

(similar to GGM construction)



(b)

$\Rightarrow PRFadv[A, F_{NR}] \leq n \cdot DDHadv[B, G]$

given g^α, g^β. difficult to distinguish between $g^{\alpha\cdot\beta}$ and g^γ $\gamma \xleftarrow{R} G$.

perfect standard DDH game. (save the proof)

10.4 (Random self-reduction for CDH (I)). Consider a specific cyclic group $\mathbb{G}$ of prime order q generated by $g \in \mathbb{G}$. For $u = g^{\alpha} \in \mathbb{G}$ and $v = g^{\beta} \in \mathbb{G}$, define $[u, v] = g^{\alpha\beta}$, which is the solution instance (u, v) of the CDH problem. Consider the randomized mapping from $\mathbb{G}^2$ to $\mathbb{G}^2$ that sends (u, v) to $(\tilde{u}, v)$, where

$$\rho \xleftarrow{R} \mathbb{Z}_q, \quad \tilde{u} \leftarrow g^{\rho} u.$$

$(u, v) \mapsto (\tilde{u}, v)$

$\rho \xleftarrow{R} \mathbb{Z}_q$.

$\tilde{u} \leftarrow g^{\rho} \cdot u = g^{\rho} \cdot g^{\alpha}$

Show that

(a) $\tilde{u}$ is uniformly distributed over $\mathbb{G}$;

(b) $[\tilde{u}, v] = [u, v] \cdot v^{\rho}$.

(a) ∵ g is a generator of $\mathbb{G}$,

→ $ord(g) = |\mathbb{G}|$

and ∵ ρ is drawn randomly.

→ $Pr[\tilde{u} = \gamma] = \frac{1}{|\mathbb{G}|}$ for $\forall \gamma \in \mathbb{G}$. ⇒ uniformly distributed

($\rho = DLog_g(\tilde{u})$)

(b) $[\tilde{u}, v] = [u, v] \cdot v^{\rho}$

∵ $[u, v] = g^{\alpha \cdot \beta}$ ⇒ $[\tilde{u}, v] = g^{(\alpha+\rho)} \cdot g^{\beta} = g^{\alpha\beta + \rho \cdot \beta}$

$[u, v] \cdot v^{\rho} = g^{\alpha \cdot \beta} (g^{\beta})^{\rho} = g^{\alpha\beta + \rho \cdot \beta} = [\tilde{u}, v]$

original: $g^{\alpha} \cdot g^{\beta} \rightarrow g^{\alpha \cdot \beta}$ CDH

↓ random self-reduction

↳ $[g^{\alpha}, g^{\beta}] \xrightarrow[R]{MAP} [g^{\rho} \cdot g^{\alpha}, g^{\beta}]$

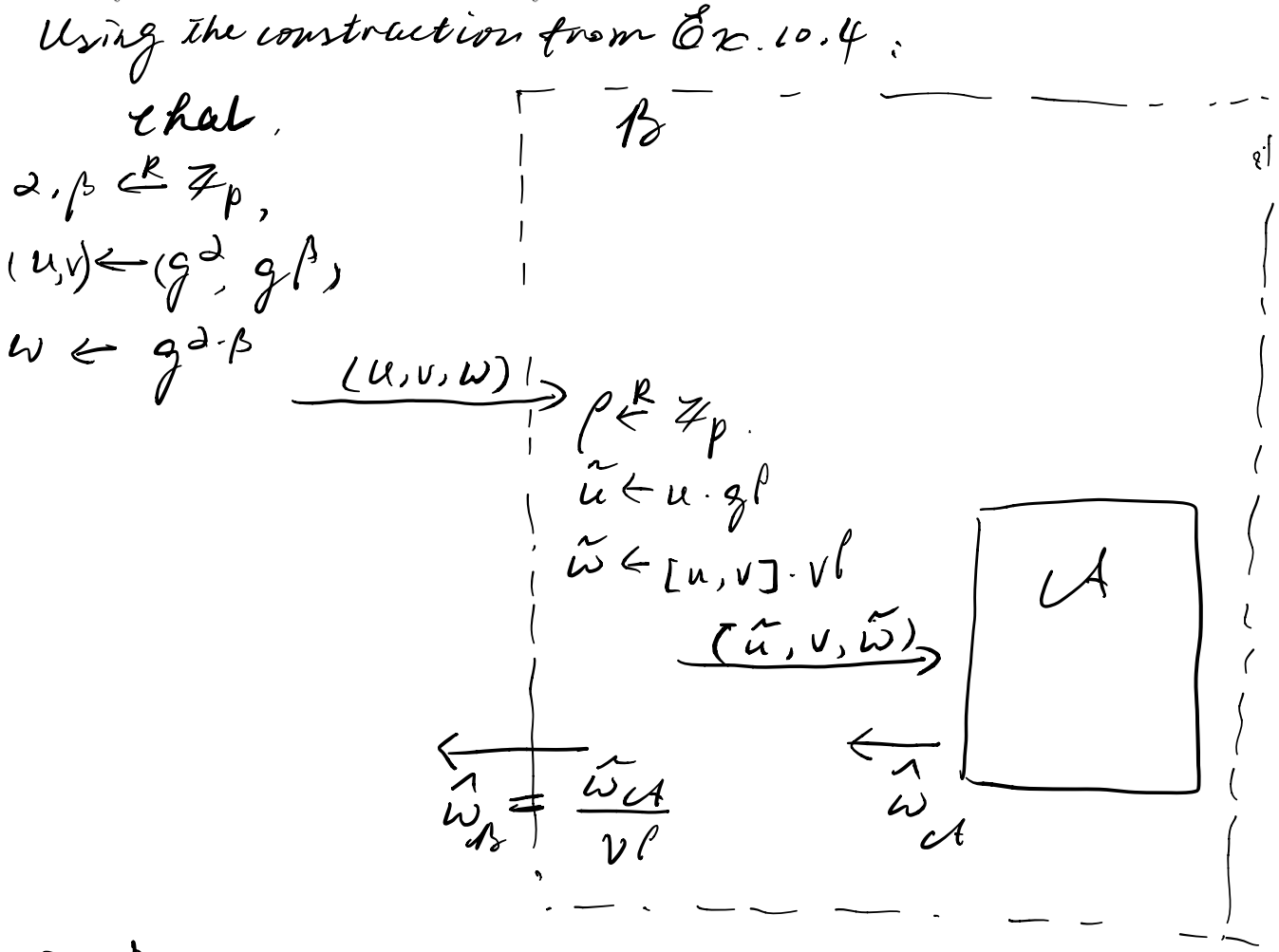
→ $g^{(\alpha+\rho)\beta}$

↓

this is randomly distributed over $\mathbb{G}$

10.5 (Random self-reduction for CDH (II)). Continuing with the previous exercise, suppose $\mathcal{A}$ is an efficient algorithm that solves the CDH problem with success probability ϵ on random inputs. That is, if $u, v \in \mathbb{G}$ are chosen at random, then $\Pr[\mathcal{A}(u, v) = [u, v]] = \epsilon$, where the probability is over the random choice of u and v, as well as any random choices made by $\mathcal{A}$. Using $\mathcal{A}$, construct an efficient algorithm $\mathcal{B}$ that solves the CDH problem with success probability ϵ for *all* inputs. More precisely, for all $u, , v \in \mathbb{G}$, we have $\Pr[\mathcal{B}(u, v) = [u, v]] = \epsilon$, where the probability is now only over the random choices made by $\mathcal{B}$.

Using the construction from Ex. 10.4:



$$\Rightarrow \Pr[\mathcal{B}(u,v) = [u,v]] = \Pr[\mathcal{A}(\tilde{u},v) = [\hat{u},v]] = \epsilon.$$

Q: CDH on $\mathbb{Z}_p$ v.s. CDH on $\mathbb{Z}_p^+$??
What are some subtleties of choosing specific groups over others?
↳ Read Boneh's DDH survey paper.

10.6 (An alternative DDH characterization). Let $\mathbb{G}$ by a cyclic group of prime order q generated by $g \in \mathbb{G}$. Let $\mathcal{P}$ be the uniform distribution over $\mathbb{G}^3$. Let $\mathcal{P}_{\text{dh}}$ be the uniform distribution over the set of all DH-triples $(g^\alpha, g^\beta, g^{\alpha\beta})$. Let $\mathcal{P}_{\text{ndh}}$ be the uniform distribution over the set of all non-DH-triples $(g^\alpha, g^\beta, g^\gamma), \gamma \neq \alpha\beta$.

(a) Show that the statistical distance (as in Definition 3.5) between $\mathcal{P}$ and $\mathcal{P}_{\text{ndh}}$ is $1/q$.

(b) Using part (a), deduce that under the DDH assumption, the distributions $\mathcal{P}_{\text{dh}}$ and $\mathcal{P}_{\text{ndh}}$ are computationally indistinguishable (as in Definition 3.4). In partcular, show that for every adversary $\mathcal{A}$, we have $\text{Distadv}[\mathcal{A}, \mathcal{P}_{\text{dh}}, \mathcal{P}_{\text{ndh}}] \leq \text{DDHadv}[\mathcal{A}, \mathbb{G}] + 1/q$.

(a)

$P: (g^\alpha, g^\beta, g^\rho)$ where α, β, ρ are independently randomly chosen from $\mathbb{G}_q$.

$P_{dh} = (g^\alpha, g^\beta, g^{\alpha\cdot\beta})$

$P_{ndh} = (g^\alpha, g^\beta, g^\gamma)$, $\gamma \neq \alpha\cdot\beta$.

Lesson: (in) distinguishability should always comes down to "statistical distance".

Definition 3.5. *Suppose P_0 and P_1 are probability distributions on a finite set $\mathcal{R}$. Then their* ***statistical distance*** *is defined as*

$$\Delta[P_0, P_1] := \frac{1}{2}\sum_{r \in \mathcal{R}} |P_0(r) - P_1(r)|.$$

Theorem 3.10. *Let P_0 and P_1 be probability distributions on a finite set $\mathcal{R}$. Then we have*

$$\max_{\mathcal{R}' \subseteq \mathcal{R}} |P_0[\mathcal{R}'] - P_1[\mathcal{R}']| = \Delta[P_0, P_1],$$

where the maximum is taken over all subsets $\mathcal{R}'$ of $\mathcal{R}$.

$$\Delta[P, P_{ndh}] = \frac{1}{2}\sum_{(u,v,w)} |P(u,v,w) - P_{ndh}(u,v,w)|$$

$\because$ for any fixed $u.v$. they're equally distributed & identical in distribution.

$$\rightarrow \Delta[P, P_{ndh}] = \frac{1}{2}\left\{ \sum_{w \neq g^\alpha \cdot g^\beta} \left|\frac{q-1}{q} - 1\right| + \sum_{w = g^\alpha \cdot g^\beta} \left|\frac{1}{q} - 0\right| \right\}$$

$$= \frac{1}{2} \cdot \left\{ \frac{1}{q} + \frac{1}{q} \right\} = \frac{1}{q}$$

(b)

Definition 3.4 (Computational indistinguishability). *Distributions P_0 and P_1 are called* ***computationally indistinguishable*** *if the value $\text{Distadv}[\mathcal{A}, P_0, P_1]$ is negligible for all efficient adversaries $\mathcal{A}$.*

$$\text{Distadv}[\mathcal{A}, P_{dh}, P_{ndh}] \leq \Delta[P_{dh}, P_{ndh}] \leq$$

$$|\Delta[P_{dh}, P]| + \Delta[P, P_{ndh}] \leq \text{DDHadv}[\mathcal{A}, \mathbb{G}] + \frac{1}{q}$$

10.7 (Random self-reduction for DDH (I)). Consider a specific cyclic group $\mathbb{G}$ of prime order q generated by $g \in \mathbb{G}$. Let **DH** be the set of all DH-triples, i.e.,

$$\mathbf{DH} := \{(g^\alpha, g^\beta, g^{\alpha\beta}) \in \mathbb{G}^3 : \alpha, \beta \in \mathbb{Z}_q\}.$$

For fixed $u \in \mathbb{G}$, and let $\mathbf{T}_u$ be the subset of $\mathbb{G}^3$ whose first coordinate is u. Consider the randomized mapping from $\mathbb{G}^3$ to $\mathbb{G}^3$ that sends (u, v, w) to (u, v^*, w^*), where

$$\sigma \xleftarrow{R} \mathbb{Z}_q, \quad \tau \xleftarrow{R} \mathbb{Z}_q, \quad v^* \leftarrow g^\sigma v^\tau, \quad w^* \leftarrow u^\sigma w^\tau.$$

Prove the following:

(a) if $(u, v, w) \in \mathbf{DH}$, then (u, v^*, w^*) is uniformly distributed over $\mathbf{DH} \cap \mathbf{T}_u$;

(b) if $(u, v, w) \notin \mathbf{DH}$, then (u, v^*, w^*) is uniformly distributed over $\mathbf{T}_u$.

(a) $u \leftarrow g^\alpha$, $v \leftarrow g^\beta$, $w \leftarrow g^{\alpha\cdot\beta}$

$u \leftarrow g^\alpha$

$v^* \leftarrow g^\sigma \cdot v^\tau = g^{\sigma+\beta\tau}$.

$w^* \leftarrow u^\sigma \cdot w^\tau = (g^\alpha)^\sigma \cdot (g^{\alpha\cdot\beta})^\tau = g^{\alpha(\sigma+\beta\tau)}$ $\Rightarrow (u, v^*, w^*) \in \mathrm{DH}$

$\because \sigma$ & τ are randomly chosen from $\mathbb{Z}_q$.

$\therefore v^*, w^*$ are all randomly / uniformly distributed over $\mathbb{G}$.

$\hookrightarrow (u, v^*, w^*)$ over $\mathrm{DH} \cap T_u$

(b) if $(u, v, w) \notin \mathrm{DH}$, Then $(u, v^*, w^*) \notin \mathrm{DH}$. , but since v^*, w^* still uniform over $\mathbb{G}$,

$\hookrightarrow (u, v^*, w^*)$ uniform over T_u.

10.8 (Random self-reduction for DDH (II)). Continuing with the previous exercise, consider the randomized mapping from $\mathbb{G}^3$ to $\mathbb{G}^3$ that sends (u, v, w) to $(\tilde{u}, v, \tilde{w})$, where

$$\rho \xleftarrow{R} \mathbb{Z}_q, \quad \tilde{u} \leftarrow g^\rho u, \quad \tilde{w} \leftarrow v^\rho w.$$

Prove the following:

(a) $\tilde{u}$ is uniformly distributed over $\mathbb{G}$; similar to Ex.10.7

(b) $(u, v, w) \in \mathbf{DH} \iff (\tilde{u}, v, \tilde{w}) \in \mathbf{DH}$; $\rightarrow$ trivial correctness proof.

(c) if we apply the randomized mapping from the previous exercise to $(\tilde{u}, v, \tilde{w})$, obtaining the triple $(\tilde{u}, v^*, \tilde{w}^*)$, then we have

- if $(u, v, w) \in \mathbf{DH}$, then $(\tilde{u}, v^*, \tilde{w}^*)$ is uniformly distributed over **DH**;
- if $(u, v, w) \notin \mathbf{DH}$, then $(\tilde{u}, v^*, \tilde{w}^*)$ is uniformly distributed over $\mathbb{G}^3$.

$(u, v, w) \longrightarrow (\tilde{u}, v, \tilde{w}) \longrightarrow (\tilde{u}, v^*, \tilde{w}^*)$

transitivity for correctness.

all are randomized over $\mathbb{G}$.

$\rightarrow (\tilde{u}, v^*, \tilde{w}^*)$. uniform over DH

otherwise, if $(u, v, w) \notin \mathrm{DH}$, Then $(\tilde{u}, v^*, \tilde{w}^*)$ is completely random & independent of each other.

$\hookrightarrow$ uniform over $\mathbb{G}^3$.

10.9 (Random self-reduction for DDH (III)). Continuing with the previous exercise, prove the following. Suppose $\mathcal{A}$ is an efficient algorithm that takes as input three group elements and outputs a bit, and which satisfies the following property: if $\alpha, \beta, \gamma \in \mathbb{Z}_q$ are chosen at random, then

$$\left|\Pr[\mathcal{A}(g^\alpha, g^\beta, g^{\alpha\beta}) = 1] - \Pr[\mathcal{A}(g^\alpha, g^\beta, g^\gamma) = 1]\right| = \epsilon,$$ ← non-negligible.

where the probability is over the random choice of α, β, γ, as well as any random choices made by $\mathcal{A}$. Assuming that $1/\epsilon$ is poly-bounded, show how to use $\mathcal{A}$ to build an efficient algorithm $\mathcal{B}$ that for all inputs (u, v, w) correctly decides whether or not $(u, v, w) \in \mathbf{DH}$ with negligible error probability. That is, adversary $\mathcal{B}$ may output an incorrect answer, but for all inputs, the probability that its answer is incorrect should be negligible.

Hint: Use a Chernoff bound.

let $\mathcal{B}$ run the composite reduction in Ex.10.8(c). s.t. if $(u,v,w) \in DH$, then $(\hat{u}, v^*, \tilde{w}^*)$ is uniformly distributed over DH.

NOTE: Markov's bound: $\Pr[X \geq a] \leq \frac{Exp[X]}{a}$ non-negative

Chebshev's bound: $\Pr[|X - Exp[X]| \geq a] \leq \frac{Var(X)}{a^2}$

Chernoff bound:

let $T_1, T_2, \cdots T_n \in [0,1]$ mutually independent.

$T = \sum_{i=1}^{n} T_i$, for any $c > 1$, $\Pr\left[\Sigma T_i \geq c \cdot Exp(\Sigma T_i)\right] \leq e^{-z\, Exp(\Sigma T_i)}$

where $z = c \cdot \ln(c) + 1 - c > 0$.

let P_i = Prob. of $\mathcal{A}$ outputting (in) correct answer. we know $Exp[\sum_{i=1}^{n} P_i] = n \cdot \epsilon$ $(1-\epsilon)$

↳ for Q queries: the prob. of $\mathcal{B}$ outputs are all incorrect:

$$\Pr[\Sigma P_i \geq c \cdot Q(1-\epsilon)] \leq e^{-zQ(1-\epsilon)}$$

for $c = \frac{1}{Q(1-\epsilon)}$ $\quad e^{-zQ(1-\epsilon)} = e^{-\left[\frac{1}{Q(1-\epsilon)} \cdot \ln(Q\cdot(1-\epsilon)) + 1 - Q(1-\epsilon)\right]Q(1-\epsilon)}$

$$= e^{-\ln(Q(1-\epsilon)) + 1 - Q(1-\epsilon)}$$

↗ negligible

10.10 (Multi-DDH (I)). Let $\mathbb{G}$ be a cyclic group of prime order q generated by $g \in \mathbb{G}$. Let n and m be positive integers. Define the following two distributions over $\mathbb{G}^{n+2nm}$:

$$\mathcal{D}: \quad g^{\alpha_i} \quad (i = 1, \ldots, n), \qquad g^{\beta_{ij}}, \quad g^{\alpha_i \beta_{ij}} \quad (i = 1, \ldots, n, \quad j = 1, \ldots, m),$$

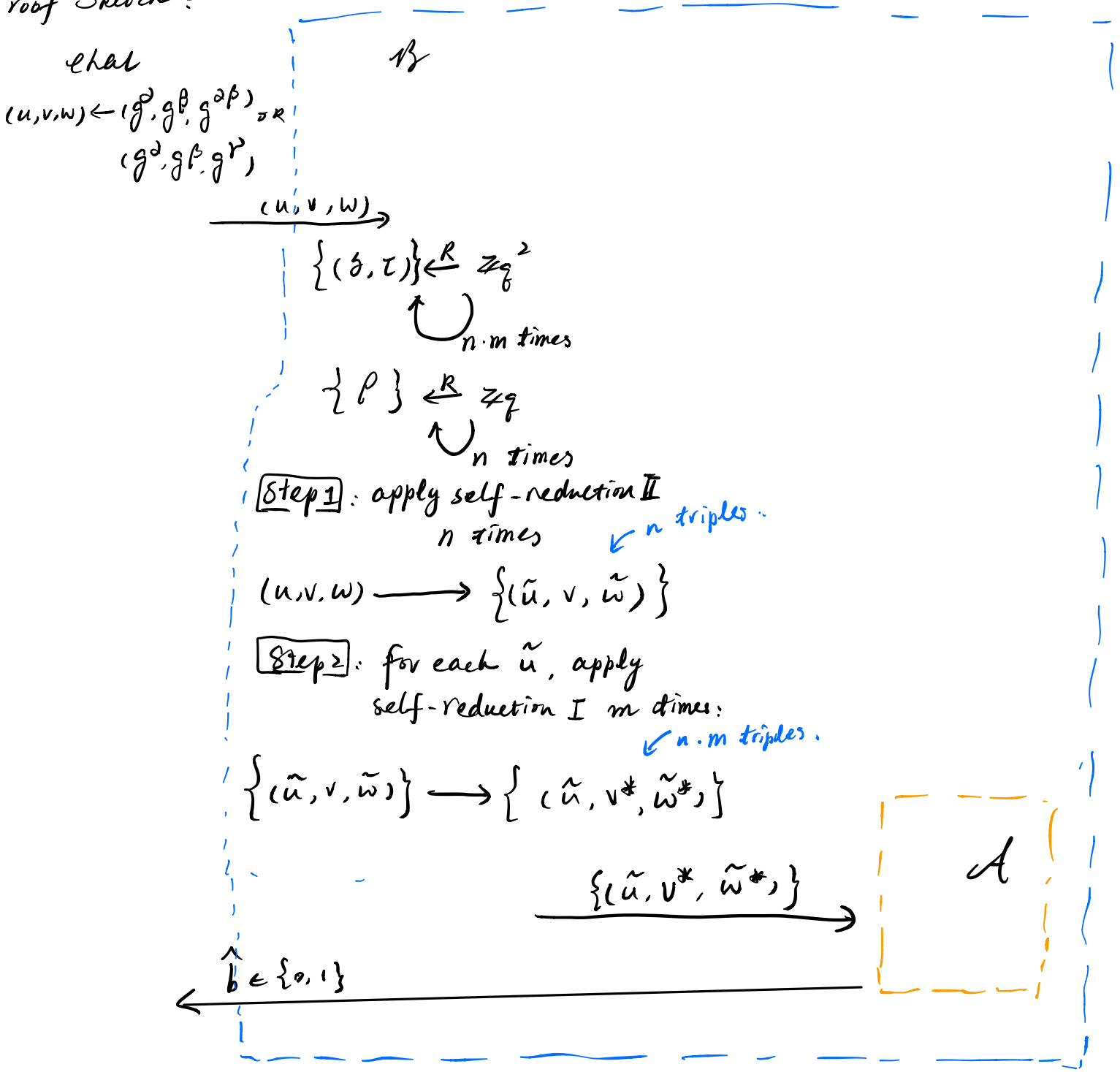
and

$$\mathcal{R}: \quad g^{\alpha_i} \quad (i = 1, \ldots, n), \qquad g^{\beta_{ij}}, \quad g^{\gamma_{ij}} \quad (i = 1, \ldots, n, \quad j = 1, \ldots, m).$$

where the α_i's, β_{ij}'s, and γ_{ij}'s are uniformly and independently distributed over $\mathbb{Z}_q$. Show that under the DDH assumption, $\mathcal{D}$ and $\mathcal{R}$ are computationally indistinguishable (as in Definition 3.4). In particular, show that for every adversary $\mathcal{A}$ that distinguishes $\mathcal{D}$ and $\mathcal{R}$, there exists a DDH adversary $\mathcal{B}$ (which is an elementary wrapper around $\mathcal{A}$) such that

$$\mathsf{Distadv}[\mathcal{A}, \mathcal{D}, \mathcal{R}] \leq 1/q + \mathsf{DDHadv}[\mathcal{B}, \mathbb{G}].$$

Proof Sketch:



Based on Ex10.7, Ex10.8:

in $Exp(0)$, $b=0$, $\because (u, v, w) \in DH$, then $\{(\tilde{u}, v^*, \tilde{w}^*)\} \in D$

in $Exp(1)$, $b=1$, $\because (u, v, w) \notin DH$, then $\{(\tilde{u}, v^*, \tilde{w}^*)\} \in R$

$\rightarrow |Pr[W_0] - Pr[W_1]| = DDH\,adv[\mathcal{B}, \mathcal{G}]$

$Dist\,adv[\mathcal{A}, D, R] \leq \Delta[P_{dh}, P_{ndh}] \leq |\Delta[P_{dh} - P]| + |\Delta[P - P_{ndh}]|$

$= |Pr[W_0] - Pr[W_1]| + \frac{1}{q}$

$= DDH\,adv[\mathcal{B}, \mathcal{G}] + \frac{1}{q}$

Lesson Learned:

1. Start from simple case, $n=1$, then generalize it & add necessary transformation
2. always have start (assumption) & goal in mind, then slowly fill in the gap. (what's missing)

10.11 (Multi-DDH (II)). Let $\mathbb{G}$ be a cyclic group of prime order q generated by $g \in \mathbb{G}$. Let $n \le m$ be positive integers. Define the following two distributions over $\mathbb{G}^{n \cdot m + n + m}$:

$$\mathcal{D}: \quad g^{\alpha_i} \ (i = 1, \ldots, n), \quad g^{\beta_j} \ (j = 1, \ldots, m)$$
$$g^{\alpha_i \beta_j} \ (i = 1, \ldots, n, \ j = 1, \ldots, m),$$

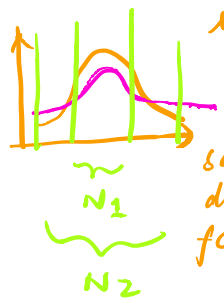
and

$$\mathcal{R}: \quad g^{\alpha_i} \ (i = 1, \ldots, n), \quad g^{\beta_j} \ (j = 1, \ldots, m)$$
$$g^{\gamma_{ij}} \ (i = 1, \ldots, n, \ j = 1, \ldots, m).$$

where the α_i's, β_j's, and γ_{ij}'s are uniformly and independently distributed over $\mathbb{Z}_q$. Show that under the DDH assumption, $\mathcal{D}$ and $\mathcal{R}$ are computationally indistinguishable (as in Definition 3.4). In particular, show that for every adversary $\mathcal{A}$ that distinguishes $\mathcal{D}$ and $\mathcal{R}$, there exists a DDH adversary $\mathcal{B}$ (which is an elementary wrapper around $\mathcal{A}$) such that

$$\mathsf{Distadv}[\mathcal{A}, \mathcal{D}, \mathcal{R}] \le n \cdot (1/q + \mathsf{DDHadv}[\mathcal{B}, \mathbb{G}]).$$

imagine:
w. $N_1 (< N_2)$ of sample, it's easier to distin ; but w more sample. The distances get flatten out



Hint: First give a proof for the case $n = 1$ using the results of Exercise 10.6 and Exercise 10.7, and then generalize to arbitrary n using a hybrid argument.

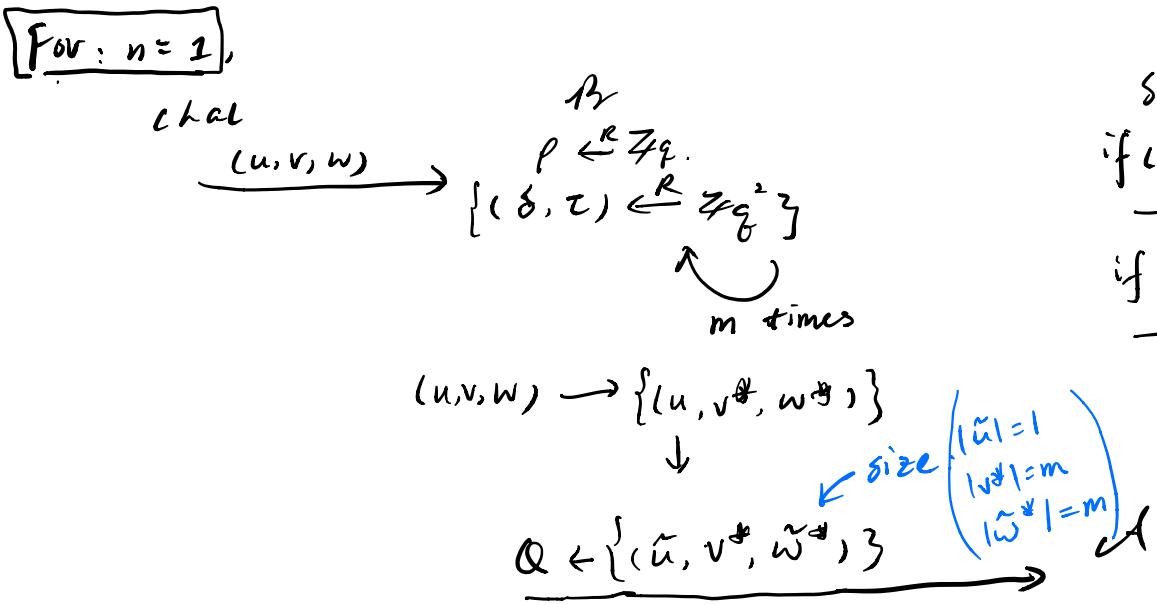
Discussion: This result gives us a DDH-based PRG G defined over $(\mathbb{Z}_q^{n+m}, \ \mathbb{G}^{n \cdot m + n + m})$, with a nice expansion rate, given by

$$G\Big(\{\alpha_i\}_{i=1}^n, \ \{\beta_j\}_{j=1}^m \Big) := \Big(\{g^{\alpha_i}\}_{i=1}^n, \ \{g^{\beta_j}\}_{j=1}^m, \ \{g^{\alpha_i \beta_j}\}_{\substack{i=1,\ldots,n \\ j=1,\ldots,m}} \Big).$$

The reader should also compare this exercise to the previous one: security in this construction degrades linearly in n, while the security in the construction in the previous exercise does not degrade at all as n increases.

intuition, in Ex 10.10, the expansion rate is terrible (< 1, actually) means that security of that comes from a growing input (sample) size

For: $n = 1$,



Similar to Ex 10.10:

if $(u, v, w) \in DH$,
$\rightarrow Q = D$
if $(u, v, w) \notin DH$,
$\rightarrow Q = R$.
$\Rightarrow$ theorem holds

For $n = i$, $i \ge 2$: proof idea: using a hybrid game construction where between 2 adjacent games, the difference $|P_k - P_{k-1}| \le \Delta[P_{dh}, P_{rdi}]$ where P_k is the prob. of certain elementary wrapper outputting the correct $\hat{b} = b$ in Hybrid game k., particularly we need:

game k:
Q_k: g^{α_i} $(i = 1, \cdots, n)$, g^{β_j} $(j = 1, \cdots, m)$, { mix of $g^{\alpha_i \beta_j}$ and $g^{\gamma_{ij}}$ }

s.t. in game 0 $(k = 0)$ { $\cdot$ } $= D$
in game n $(k = n)$ { $\cdot$ } $= R$

Proof: # Game k:

chal $\xrightarrow{(u,v,w)}$ B_0

$\{\rho\} \xleftarrow{R} Z_q$ ↷ n times

$\{(\sigma, \tau)\} \xleftarrow{R} Z_q^2$ ↷ m times

randomly generated

g^{α_i} ▭ n

g^{β_j} ▭ m

$g^{\gamma_{ij}}$ ▭ (with k) $n \times m$

for $i = 0, \cdots, k$

$(u, v, w) \longrightarrow (\tilde{u}, v, \tilde{w})$

for $i = k+1, \cdots, n$

10.12 (Matrix DDH). Let $\mathbb{G}$ be a cyclic group of prime order q generated by $g \in \mathbb{G}$. Let n and m be positive integers, and assume $n \leq m$. For $A = (\alpha_{ij}) \in \mathbb{Z}_q^{n \times m}$ (i.e., A is an $n \times m$ matrix with entries in $\mathbb{Z}_q$), let g^A be the $n \times m$ matrix whose entry at row i column j is the group element $g^{\alpha_{ij}}$. For $k = 1, \ldots, n$, define the random variable $R(k)$ to be a random matrix uniformly distributed over all $n \times m$ matrices over $\mathbb{Z}_q$ of of rank k. Let $1 \leq k_1 < k_2 \leq n$. Show that $g^{R(k_1)}$ and $g^{R(k_2)}$ are computationally indistinguishable under the DDH. In particular, show that for every adversary $\mathcal{A}$ that distinguishes $g^{R(k_1)}$ and $g^{R(k_2)}$ there exists a DDH adversary $\mathcal{B}$ (which is an elementary wrapper around $\mathcal{A}$) such that

$$\mathsf{Dist}\mathsf{adv}[\mathcal{A}, g^{R(k_1)}, g^{R(k_2)}] \leq (k_2 - k_1) \cdot (1/q + \mathrm{DDH}\mathsf{adv}[\mathcal{B}, \mathbb{G}]).$$

Hint: Use the fact that if $A \in \mathbb{Z}_q^{n \times m}$ is a fixed matrix of rank k, and if $U \in \mathbb{Z}_q^{n \times n}$ and $V \in \mathbb{Z}_q^{m \times m}$ are a random *invertible* matrices, then the matrix $UAV \in \mathbb{Z}_q^{n \times m}$ is uniformly distributed over all $n \times m$ matrices of rank k. You might also try to prove this fact, which is not too hard.

Discussion: For $k_1 = 1$ and $k_2 = n$, this result implies a closely related, but slightly weaker form of Exercise 10.11. In this sense, this exercise is a generalization of Exercise 10.11.