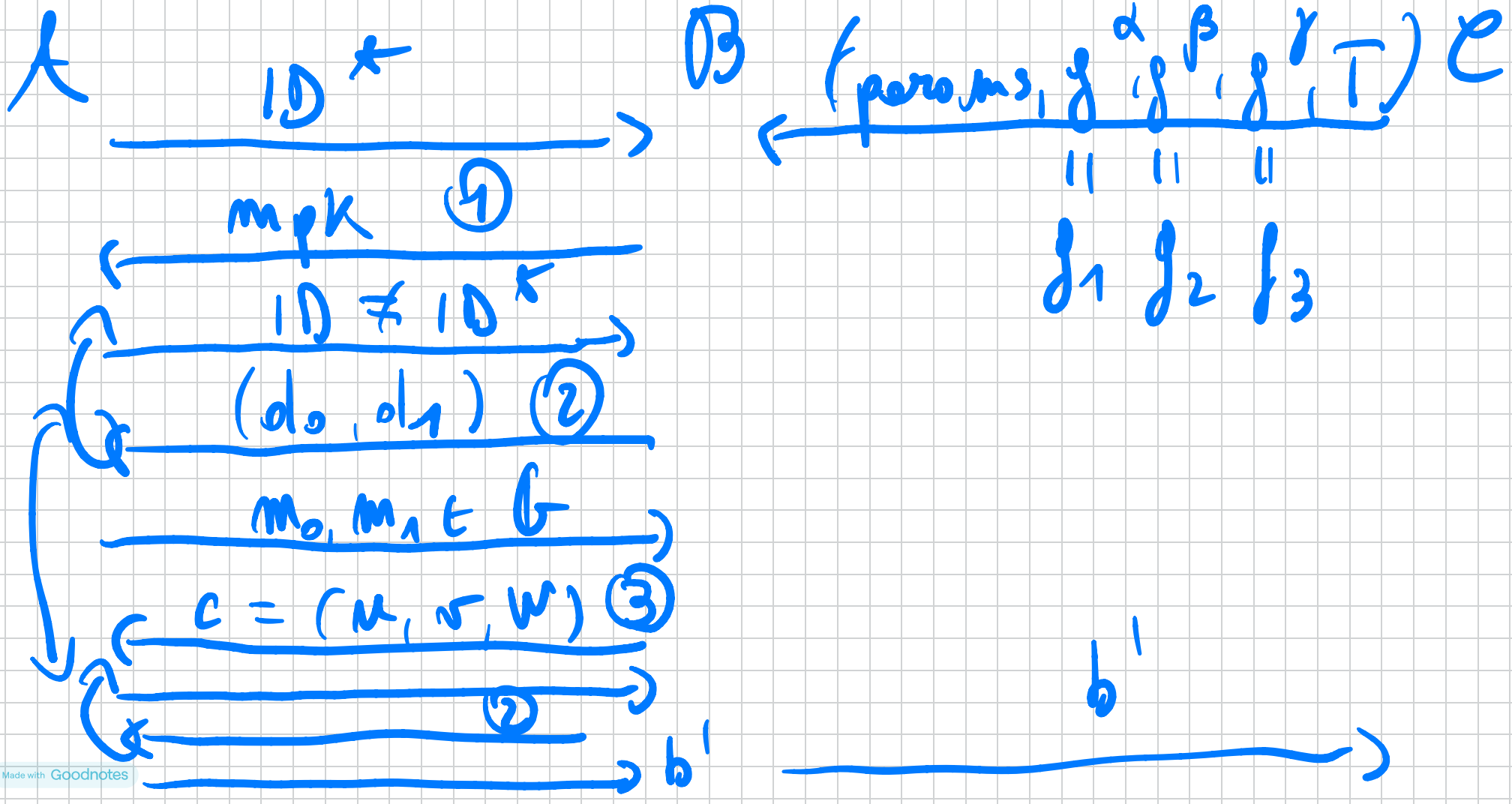
Proof. Let A be a PPT adversary breaking selective IND-ID-CPA of $\overline{\Pi}$.
We construct PPT $\mathcal{B}$ breaking DBDH.



④ $mpk. = (params, g_1, g_2, h)$

$g_1 = g^{\alpha}$, $g_2 = g^{\beta}$

$h = g_1^{-ID^*} \cdot g^{a} \in \mathbb{G}$; $a \leftarrow \mathbb{Z}_q$

(Note that $msk = g_2^{\alpha} = g^{\alpha\beta}$ is unknown to B.)

$$F(ID) = g_1^{ID} \cdot h$$

② Extraction queries $ID \neq ID^*$

$$d_{ID} = (d_0, d_1)$$

$$d_0 = g_2^{-\alpha/(ID-ID^*)} \cdot F(ID)^r \quad ; \quad r \leftarrow \mathbb{Z}_q$$

$$d_1 = \left(g^{\tilde{r}} = g^{r - \beta/(ID-ID^*)} \Rightarrow \frac{g^r}{g_2^{1/(ID-ID^*)}} \right.$$

(The original Extraction was:

$$d_1 = g^r \; ; \; d_0 = g_2^{\alpha} \cdot F(ID)^r \; . \;)$$

③ Challenge CTX : $m_0, m_1 \leftarrow G$

$$C = (u, v, w)$$

(Recall the original : $u = \hat{e}(g_1, g_2)^{\gamma}$;

$v = g^{\gamma}$, $w = F(ID^*)^{\gamma}$.)

$v = g^{\gamma}$; $u = T \cdot m_b$

$$w = g_3^{\alpha}$$

Analysis:

① The mpk is perfectly simulated.

No, $h = g_1^{-1/\alpha} \cdot g^{\alpha}$ is uniform.

③ The challenge ctx $c = (u, v, w)$.

If $T = \hat{e}(g, g)^{\alpha\beta\gamma}$ then

$u = T \cdot m_b = \hat{e}(g_1, g_2)^{\gamma} \cdot m_b$ ✓

$v = g_2^{\gamma}$ ✓

$w = g_3$

Note that $F(ID^*)^\gamma = (g_1^{ID^*} \cdot h)^\gamma =$

$= (g_1^{ID^*} \cdot g_1^{-ID^*} \cdot g^e)^\gamma = g_3^e$ ✓

② Extraction queries $ID \neq ID^*$.

$sk_{ID} = g^{\tilde{r}}$ ✓ where $\tilde{r} = r - \beta / (ID - ID^*)$

$\tilde{r}$ is still uniform.

We must prove:

$d_0 = g_2^\alpha \cdot F(ID)^{\tilde{r}}$

Well, recall:

$$o|_o = g_2^{-Q/1D-1D^*} \cdot \Gamma(|D|^r$$

$$= g_2^{-Q/1D-1D^*} \cdot \left(g_1^{1D} \cdot (g_1^{-1D^*} \cdot g^Q) \right)^r$$

$$= g_2^{-Q/1D-1D^*} \cdot \left(g_1^{1D-1D^*} \cdot g^Q \right)^r$$

$$= \left(g_1^{1D-1D^*} \cdot g^Q \right)^{\beta/1D-1D^*} \cdot \left(g_1^{1D-1D^*} \cdot g^Q \right)^r \cdot g_2^{-\frac{Q}{1D-1D^*}}$$

$$\left(g_1^{1D-1D^*} \cdot g^Q \right)^{\beta/1D-1D^*}$$

$$= g_1^{\beta} \cdot g^{\alpha\beta/10-10^k} \cdot g_2^{-\alpha/10-10^k} \cdot \left(g_1^{10-10^k} \cdot g^{\alpha} \right)^{n-\beta/10-10^k}$$

$$= \underbrace{\left(g_2^{\alpha} \right)}_{msk} \cdot \underbrace{\left(g_1^{10-10^k} \cdot g^{\alpha} \right)}_{F(10)}^{\approx}$$

✓

APPLICATIONS

We'll show 2 applications:

1) CCA-secure PKE

2) UF-CMA Signatures.

Let's start with 1. Two ingredients:

(I) $\Pi = (Setup, KGen, Enc, Dec)$ an IBE scheme.

(II) $\Pi' = (KGen', Sign, Vrfy)$

Define $\Pi'' = (Kgen'', Enc'', Dec'')$:

*) $Kgen''(1^\lambda)$: $(mpk, msk) \leftarrow Setup(1^\lambda)$

and output $ek = mpk$; $dk = msk$.

*) $Enc''(ek, m)$: Run $(\nu k, sk) \leftarrow Kgen'(1^\lambda)$

s.t. $|\nu k| = n(\lambda)$. Output:

$$c'' = (c, \nu k, \sigma)$$

$c \leftarrow Enc(mpk, ID = \nu k, m)$

$\sigma \leftarrow Sign(sk, c)$

*) $Dec''(dk, C'')$. Given $C'' = (c, vk, \sigma)$

If $Vrfy(vk, c, \sigma) = 0$ output $\perp$.

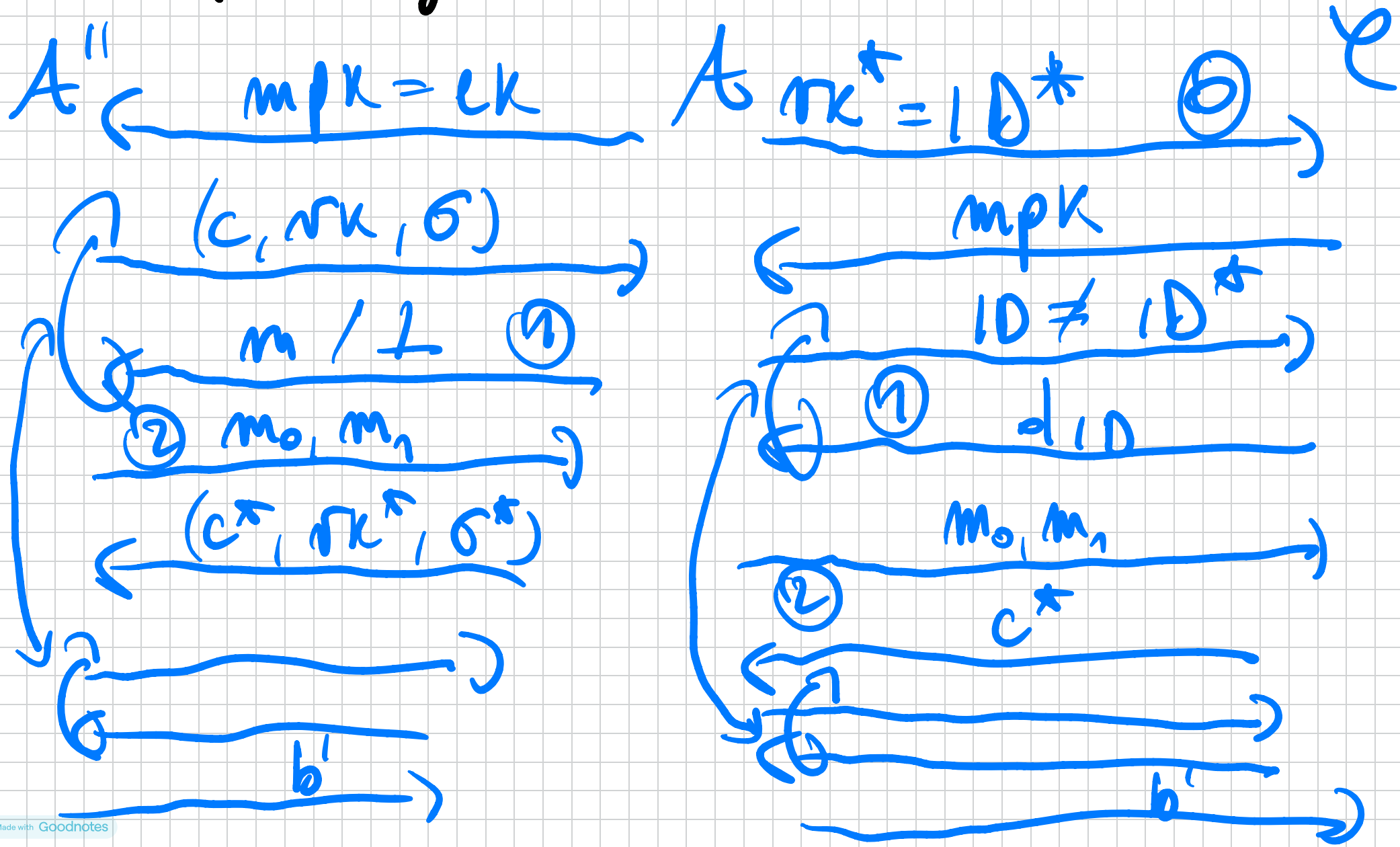
Else, output $Dec(mpk, dk_{vk}, c)$

$$dk_{vk} \leftarrow Kgen(msk, vk = ID)$$

Thm Assuming Π is selective IND-ID-CPA and Π' is strongly UF-CMA, then Π'' is CCA-secure.

Proof. We will basically give a sketch.

Assume $\exists$ PPT A'' breaking Π''. Consider the following reduction to Π.



② Given a query (c, pk, σ). First, if $Verify(pk, c, \sigma) = 0$ output $\perp$.

Else:

- If $pk \neq pk^*$ then send pk to $\mathcal{C}$, receive d_{ID} and output $Dec(mpk, d_{ID}, c)$. ✓
- If $pk = pk^*$, then we can't send $ID^* = pk^*$ to $\mathcal{C}$.

Note that $(c, \sigma) \neq (c^*, \sigma^*)$

otherwise $(c, vk, \sigma) = (c^*, vk^*, \sigma^*)$.

Then, we can just reject this query.

② Upon $m_0, m_1 \in \mathcal{M}$, then send m_0, m_1 to $\mathcal{C}$, obtain

$$c^* \leftarrow Enc(mpk, ID^* = vk^*, m_b)$$

output $\left(c^*, vk^*, \sigma^* \leftarrow Sign(sk, c^*)\right)$

The actual proof:

1) Create a hybrid where dec. queries (c, vk, σ) with $vk = vk^*$ but $(c, \sigma) \neq (c^*, \sigma^*)$ are rejected.

By UF-CMA this is indistinguishable.

2) Use the above reduction to IND-1D-CPA to show that no attacker can break CCA security in the hybrid.

We finish up by showing that IBE also implies signatures.

Let $\Pi = (\text{Setup}, \text{Kgen}, \text{Enc}, \text{Dec})$ be an IBE. Consider $\Pi' = (\text{Kgen}', \text{Sign}, \text{Vrfy})$

*) $\underline{\text{Kgen}'}(1^\lambda)$: $(mpk, msk) \leftarrow \text{Setup}(1^\lambda)$

output $vk = mpk$ and $sk = msk$.

*) $\underline{\text{Sign}}(sk, \underline{m})$: Think of $m \in ID$.

Output $\sigma = d_m \leftarrow \text{Kgen}(msk, m)$.

*) Vrfy ($\underline{vk}$, $\underline{m}$, σ) : Apart from that of $m = ID$ and $\sigma = d_{ID}$.

Pick $\mu \in M_{IBE}$ (plaintext for IBE) and let $C \in Enc(mpk, ID = m, \mu)$.

Accept (m, σ) iff $Dec(d_{ID}, C) = \mu$.

We'll show UFCMA follows from the following weak property of IBE:

OW-ID-CPA.

ow-wol-cpa

$G_{AMS}(\lambda)$:

Π, A

A

mpk

C

mpk, msk

ID

d_{ID}

$ID^* \neq ID$

Not needed in the proof

c^*

$\mu \leftarrow M_{IDS}$

$c^* \leftarrow Enc(mpk, ID^*, \mu)$

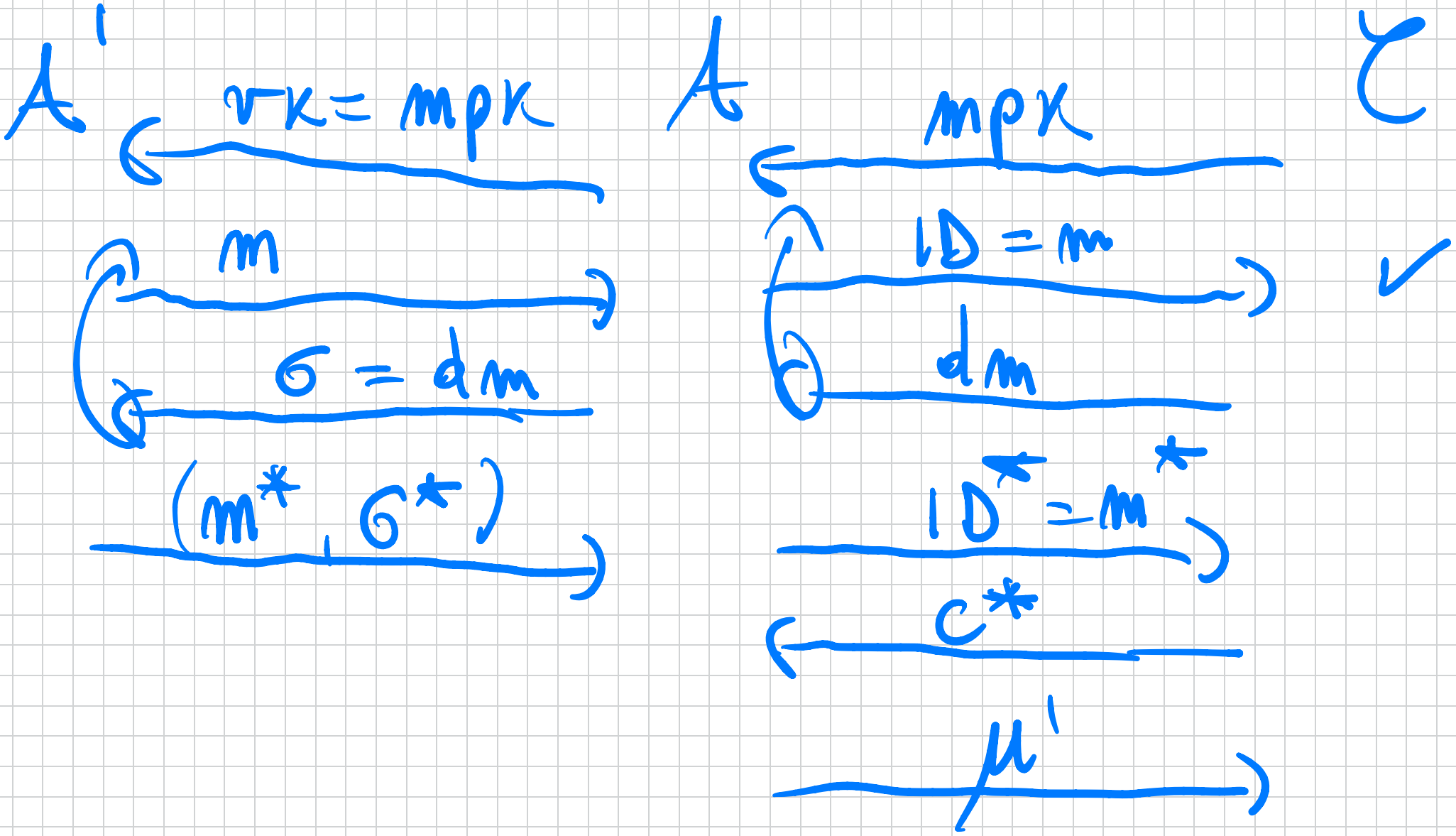
μ'

Output 1 iff $\mu' = \mu$.

We are going to need OW-ID-CPA with negligible advantage: This is implied by IND-ID-CPA + $\frac{1}{|\mathcal{M}_{IBS}|} = negl(\lambda)$.

THM Assuming Π satisfies OW-ID-CPA then Π' is UF-CMA.

Proof. Simple reduction: Assume $\exists$ PPT A' against UFCMA, we build PPT A against the IBE.



$$\mu' = Dec(mpk, \underbrace{\sigma^*}_{dm^*}, c^*)$$

$$\Pr[A \text{ wins}] \geq \Pr[A' \text{ wins}]$$

$$\geq 1/\text{poly}(\lambda)$$

Note: The reduction would in principle break in case the IBE is only selectively secure.

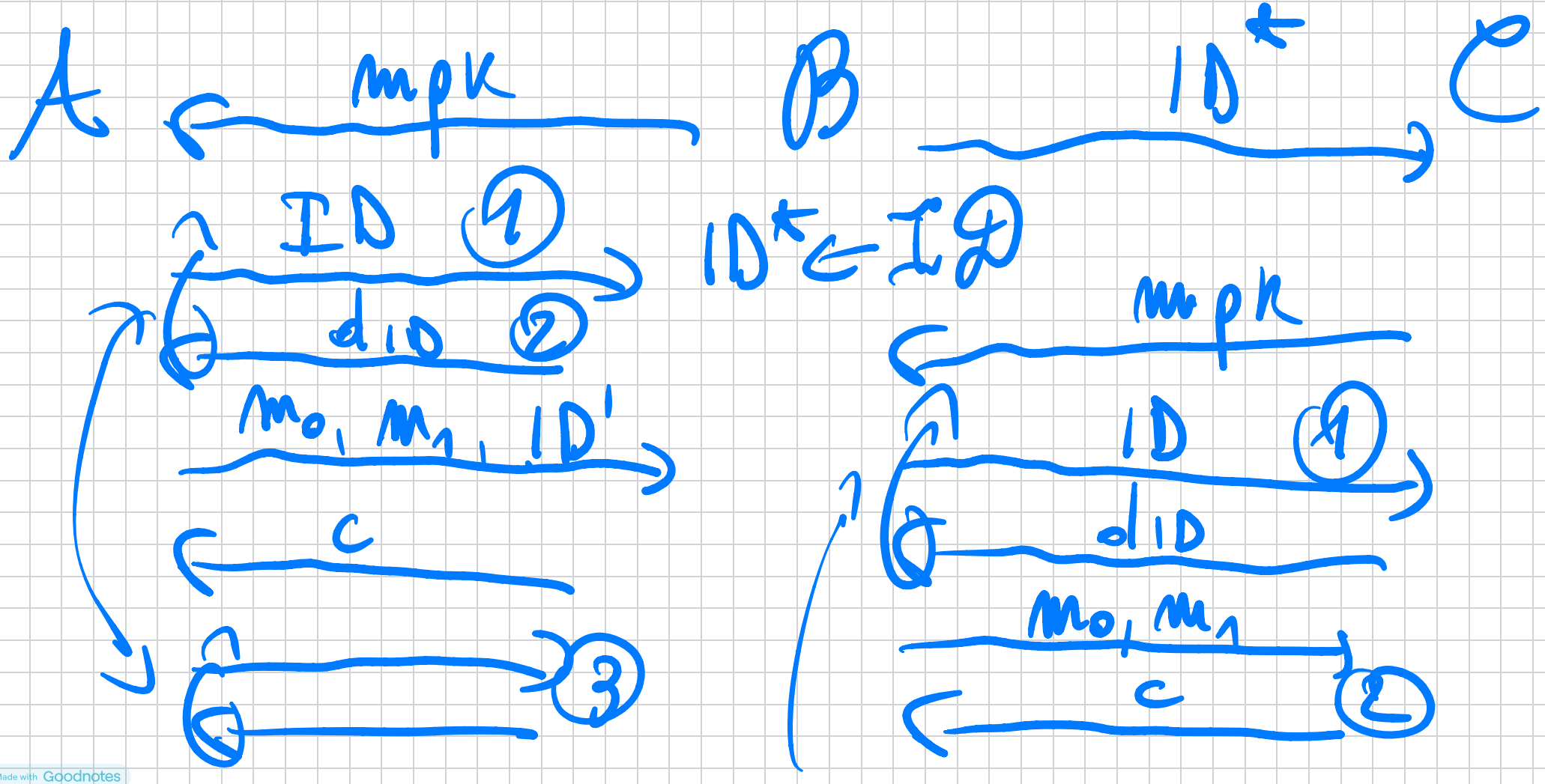
$\Rightarrow$ We need IBE to be

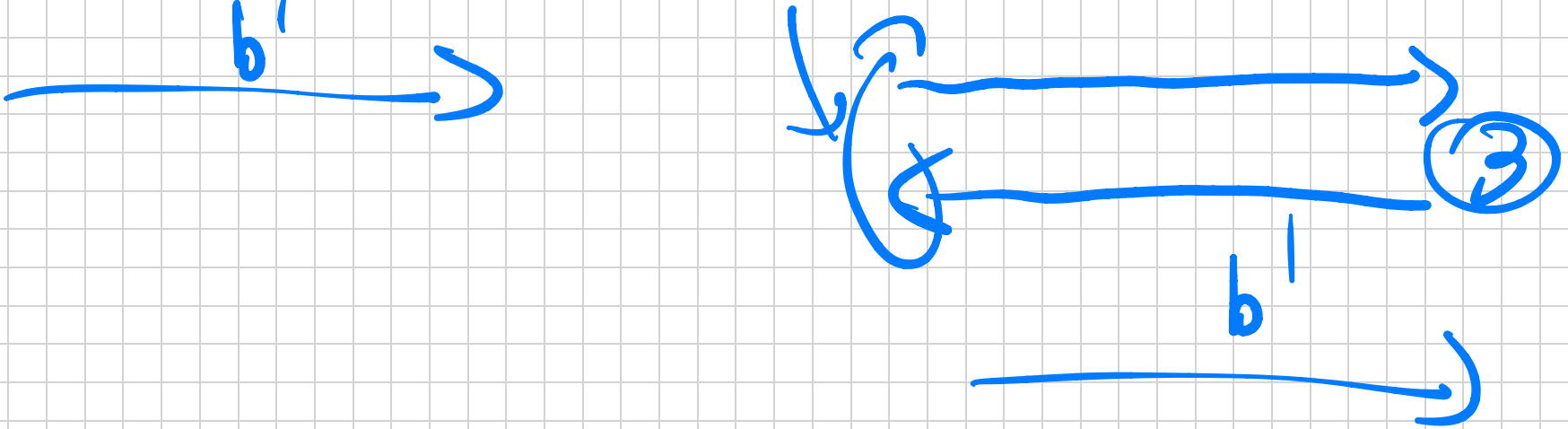
IND-ID-CPA.

Good news: While there are direct constructions, it's also true that any selective IND-ID-CPA IBE is also IND-ID-CPA with a tight loss in the parameters:

Thm Any IBE that is (t, q, ε)-selectively IND-ID-CPA is also $(t, q, N\varepsilon)$-IND-ID-CPA with $N = |ID|$

Proof sketch: given $\mathcal{A}$ breaking IND-ID-CPA game of $\mathcal{B}$ breaking the selective notion.





① If $ID = ID^*$. Abort. Else, we are good.

② If $ID' \neq ID^\Gamma$. Abort. Else, we are good.

③ Assuming we did not abort

Lemma: $ID \neq ID^*$ and we are done.

$q_1 = q$ # (1) queries

$$\Pr[\neg ABORT] \geq \left(1 - \frac{q_1}{N}\right) \cdot \frac{1}{N - q_1}$$

$$= 1/N$$

$\Rightarrow$ The distinguishing advantage is $\geq \varepsilon/N$. ∎