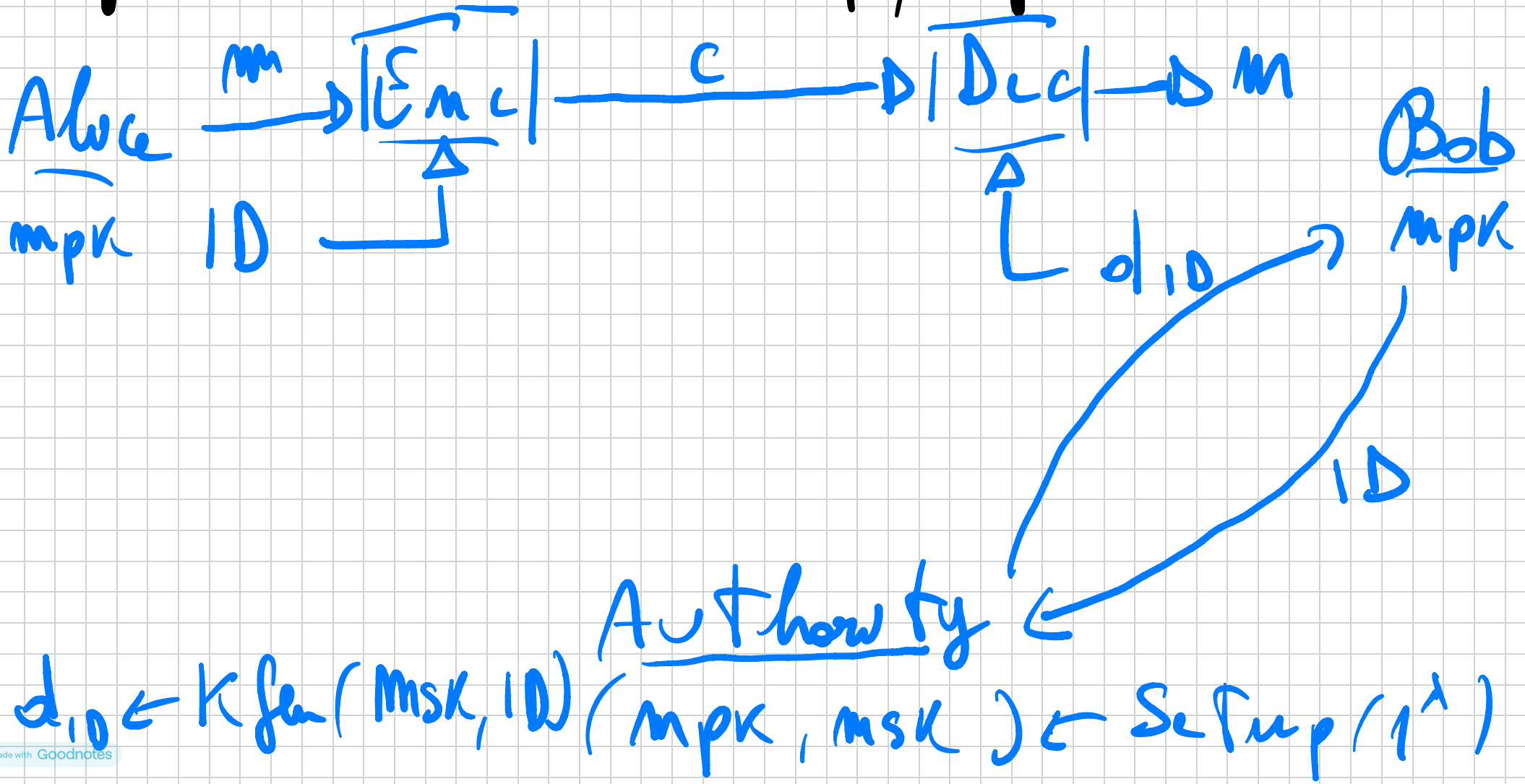
IDENTITY - BASED ENCRYPTION

IBE: Public-key encryption where the pk can be an arbitrary string. Why is it useful? If we can associate unique identities to people (e.g. social security number), we can encrypt only knowing an ID ∈ {0,1}*

Since we need to generate secret keys we need an authority anyway.

because otherwise everybody could generate secret keys for arbitrary IDs.

Syntax: $\Pi = (\text{Setup}, \text{KGen}, \text{Enc}, \text{Dec})$.



Key escrow: It's a new issue. The authority can generate all secret keys. So, it can decrypt everything.

Advantage: No certificates. Zero overhead.

Why is it interesting?

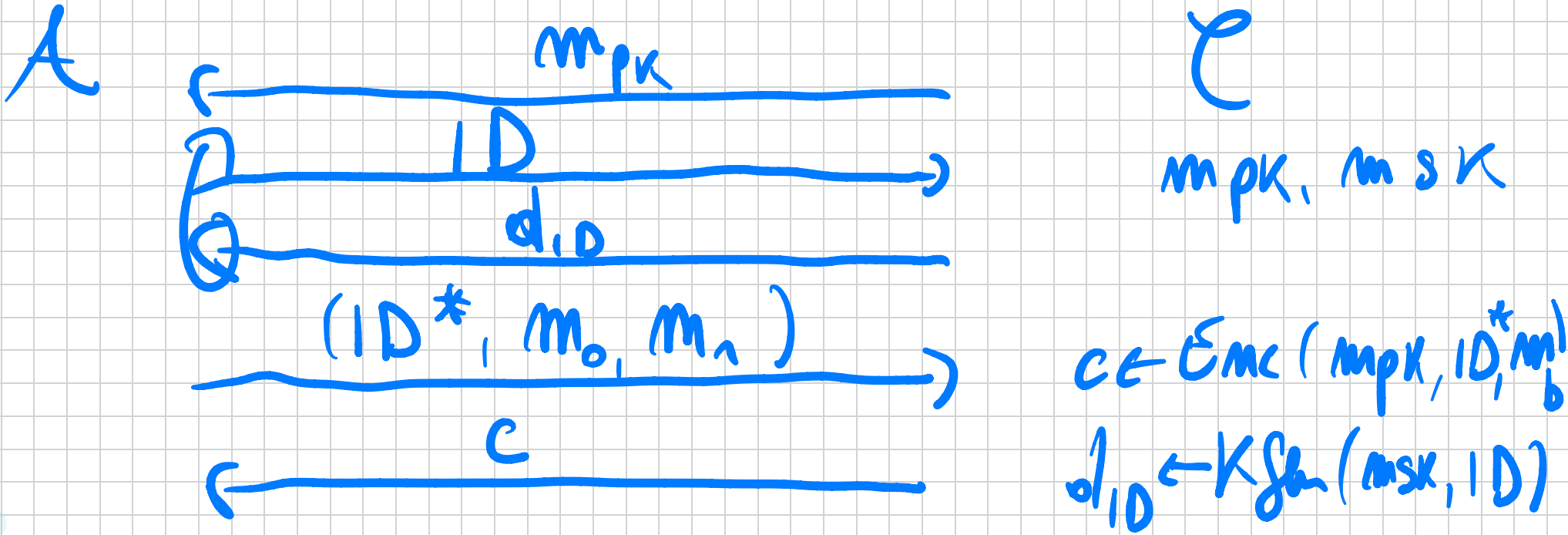
- A generalization of PKE. With further generalizations one gets new forms of encryption that are more expressive than PKE: ABE, Functional encryption

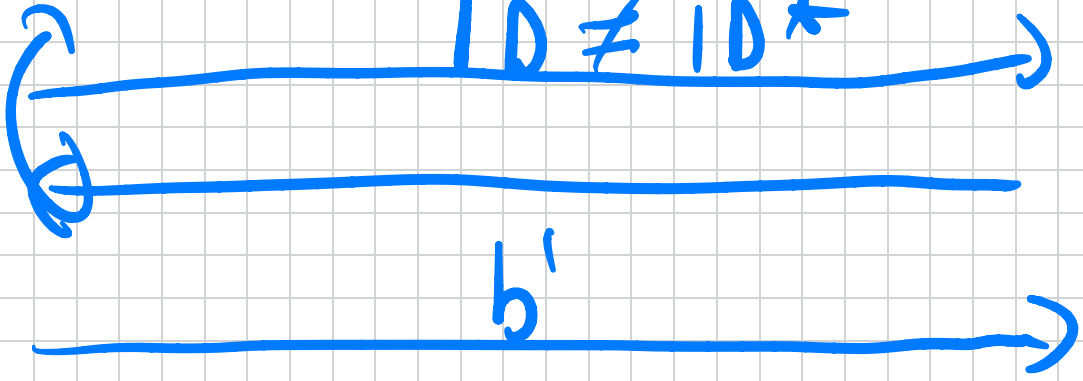
...

- We'll show that IBE implies both: Digital signatures, CCA-secure PKE.

Security: IND-ID-CPA security.

$\text{GAME}^{\text{id-cpa}}_{\Pi,\mathcal{A}}(\lambda, b)$





Next goal: A construction of IBE. The construction will satisfy a weaker definition. This version is called SELECTIVE IND-ID-CPA: This means A picks ID^* before mpk is sampled. Selective will be enough for us and the mentioned applications!

The construction: It will be based on so-called pairings. We will write:

$(\underline{G}, \underline{G_T}, \underline{g}, \underline{q}, \underline{\hat{e}}) \leftarrow$ group gen(1^λ)

(i) G is cyclic with generator g and order q (prime).

(ii) $\hat{e} : G \times G \longrightarrow G_T$ such that:

$\forall\, g, h \in G,\ \forall\, a, b \in \mathbb{Z}_q$

$$\hat{e}(g^a, h^b) = \hat{e}(g, h)^{ab}$$

(G_T is also of prime order q.)

Example: $\hat{e}$ exists in elliptic curve groups.

Consequence: DDH does not hold in bilinear groups. Given g^a, g^b, g^c:

$$\hat{e}(g, g^c) = \hat{e}(g^a, g^b)$$

$$\left(= \hat{e}(g,g)^{abc}\right)$$

Here is an assumption that is believed to hold:

DEP (DBDH) For $a,b,c \leftarrow \mathbb{Z}_q$, $T \in G_T$

$$\left(g^a, g^b, g^c, \hat{e}(g,g)^{abc}\right) \approx_c$$

$$\left(g^a, g^b, g^c, T\right)$$

The construction:

*) Setup(1^λ): $(\underbrace{G, G_T, g, q, \hat{e}}_{\text{params}}) \leftarrow \text{GroupGen}$.

Pick $h \leftarrow G$, $g_2 \leftarrow G$ and $g_1 = g^\alpha$ for $\alpha \leftarrow \mathbb{Z}_q$. Then:

$mpk = (\text{params}, g, g_1, g_2, h)$

$msk = g_2^\alpha$

*) KGen (msk, ID) : Consider $F: \mathbb{Z}_q \to G$

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

Given $ID \in \mathbb{Z}_q$, pick $r \in \mathbb{Z}_q$ and output $d_{ID} = (d_0, d_1)$

$$d_0 = \underbrace{g_2^{\alpha}}_{msk} \cdot F(ID)^r, \; d_1 = g^r$$

(Using $H: \{0,1\}^* \to \mathbb{Z}_q$ we extend the $ID \in \{0,1\}^*$.)

*) Enc (mpk, ID, m) : given $m \in G_T$, pick $r \leftarrow \mathbb{Z}_q$ and output

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

$$u = \hat{e}(g_1, g_2)^r \cdot m$$

$$v = g^r$$

$$w = F(ID)^r$$

*) $\underline{\text{Dec}}(\underline{mpk}, \underline{d_{ID}}, \underline{c})$: Parse $c = (u, v, w)$ and $d_{ID} = (d_0, d_1)$. Then output:

$$\frac{u \cdot \hat{e}(d_1, w)}{\hat{e}(v, d_0)} =$$

$$\hat{e}(g_1, g_2)^{\gamma} \cdot m \cdot \frac{\hat{e}(g^{r}, F(ID)^{\gamma})}{\hat{e}(g^{\gamma}, g_2^{\alpha} \cdot F(ID)^{r})} =$$

$$\frac{\hat{e}(g_1, g_2)^{\gamma} \cdot m \cdot \hat{e}(g, F(ID))^{r\cdot\gamma}}{\hat{e}(g^{\gamma}, g_2^{\alpha}) \cdot \hat{e}(g^{\gamma}, F(ID)^{r})}$$

$$= \hat{e}(g^{\alpha}, g_2^{\gamma})$$

$$= \hat{e}(g_1, g_2)^{\gamma}$$

Teo The above IBE is selective IND-ID-CPA under the DBDH assumption.