PRFs. Apply GGM with a particular PRG. We get:

$$\mathcal{F} = \left\{ F_{\vec{e}} : \{0,1\}^n \to G \right\}_{\vec{e} \in \mathbb{Z}_q^{n+1}}$$

$$F_{\vec{e}}(0\,1) = g^{e_0 \cdot e_1^0 e_2^1} = g^{e_0 e_2}$$

(x_1 selects e_1^0, x_2 selects e_2^1)

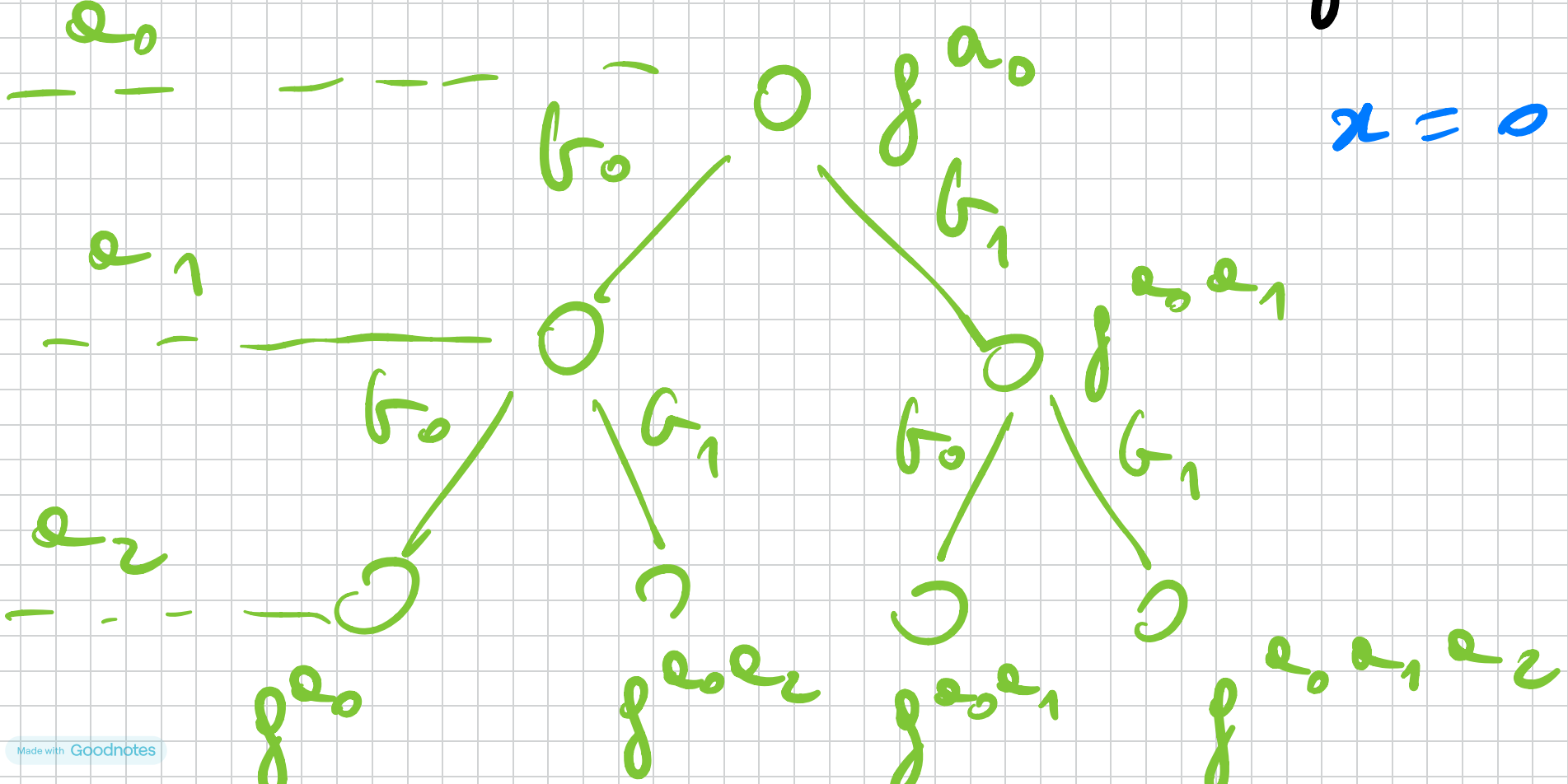
$$F_{\vec{e}}(x_1, \dots, x_n) = \left(g^{e_0}\right)^{\prod_{i=1}^{n} e_i^{x_i}}$$

The above is GRM with following PRG:

$$G_a(g^b) = (g^b, g^{ab})$$

$$= G_0(g^b) \| G_1(g^b)$$

$x = 01$



*) CRH simple construction from DL over (G, g, q) q is a prime.

$$H_{g_1 g_2}(x_1, x_2) = g_1^{x_1} g_2^{x_2} \text{ in } G$$

(e.g. $G = QR_p$ s.t. $\frac{p-1}{2} = q$.)

$g_1 = g$ the generator.

$g_2 =$ ANY group element.

$H : \mathbb{Z}_q^2 \to G$ is RANDOM.

Given a collision (x_1, x_2), (x_1', x_2') s.t. $(x_1, x_2) \neq (x_1', x_2')$ and

$$g_1^{x_1} g_2^{x_2} = g_1^{x_1'} g_2^{x_2'}$$

$$g_1^{x_1 - x_1'} = g_2^{x_2' - x_2}$$

$$g_2 = g_1^{(x_1 - x_1')(x_2' - x_2)^{-1}}$$

$x_2' \neq x_2$ then the inverse exists.

(Note that if $x_2 = x_2'$ then also $x_1 = x_1'$.)

$\Rightarrow (x_1 - x_1')(x_2' - x_2)^{-1}$ is the DL of g_2.

$A_{CRI+} \leftarrow (G, g_1 = g_1, g_2 = y_{1,q})$

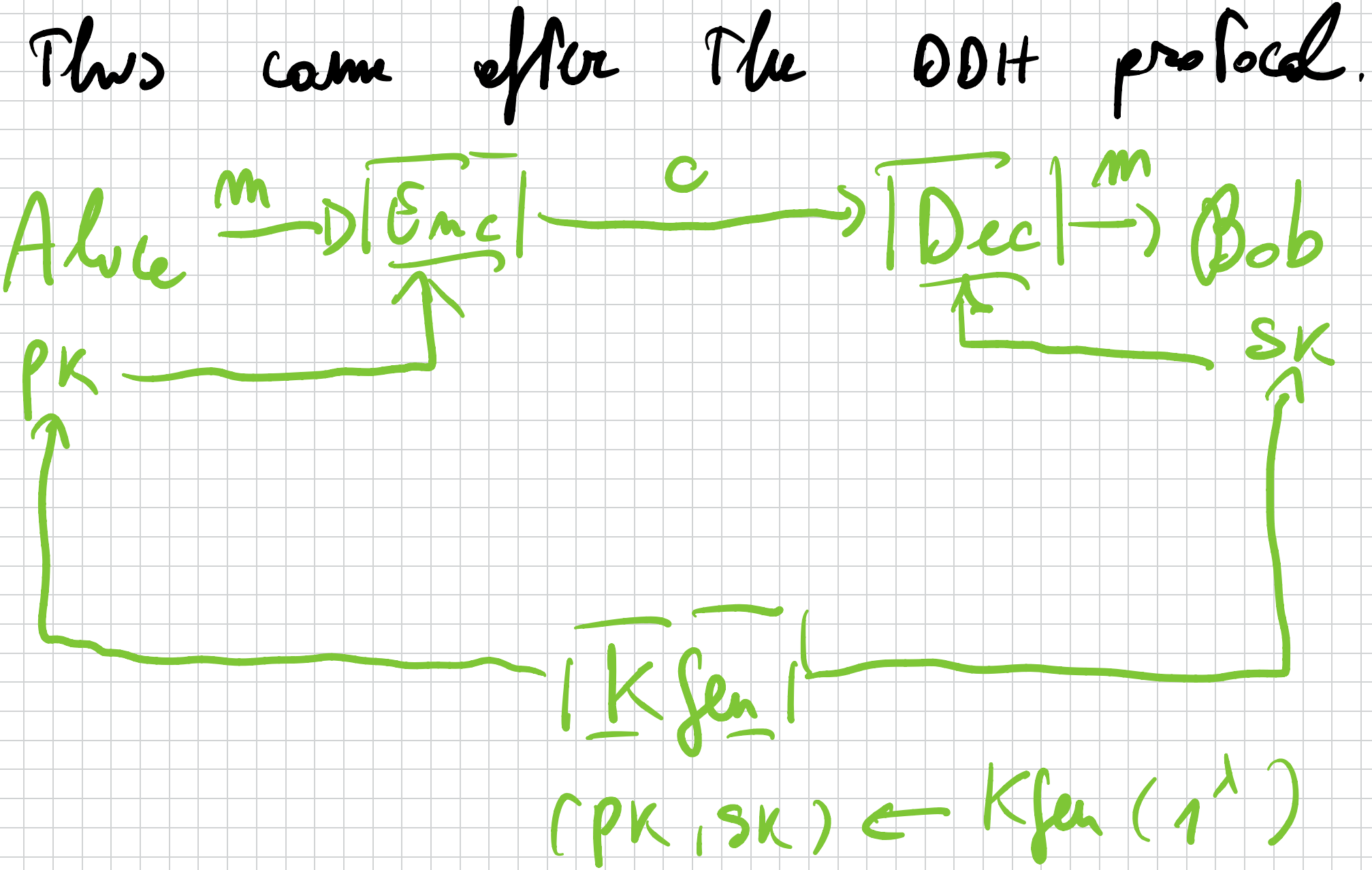
$A_{DL} \leftarrow$ params y, $= (G, g, q)$

C_{DL}: $y = g^x$, $x \leftarrow \mathbb{Z}_q$, $(x_1 - x_1')(x_2' - x_2)^{-1}$

x_1, x_2, x_1', x_2'

PUBLIC-KEY ENCRYPTION

This came after the DDH protocol.

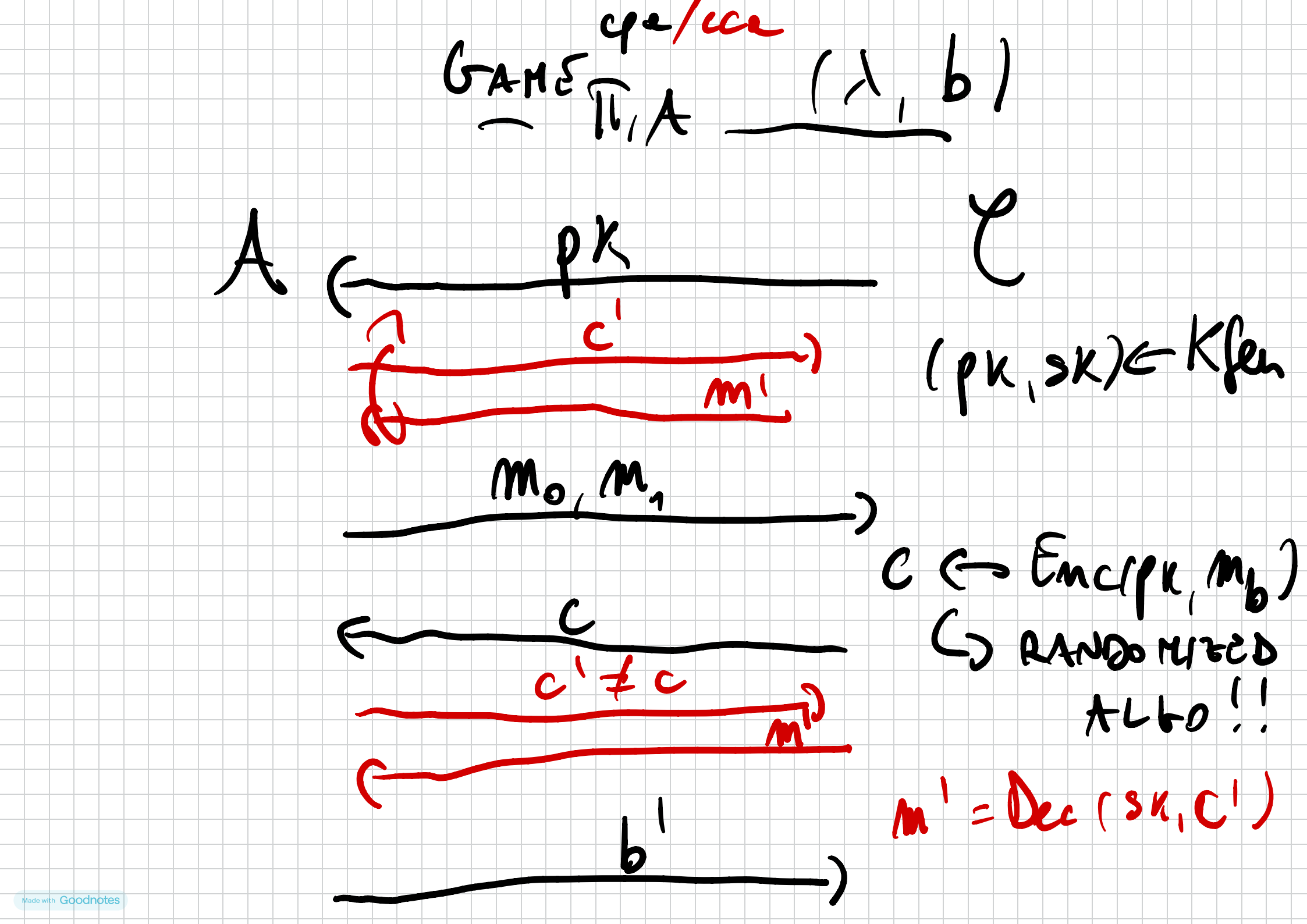


We are neglecting a problem: Alice should know pk_B as the public key of Bob. How to do that: DIGITAL SIGNATURES and PKI.

Security: CPA / CCA

DEF $\Pi = (Kgen, Enc, Dec)$ as CPA/CCA secure if

$$GAME^{cpa/cca}_{\Pi,A}(\lambda, 0) \approx_c GAME^{cpa/cca}_{\Pi,A}(\lambda, 1).$$


CPA/CCA
GAME Π, A
(λ, b)
A
pk
C
c'
m'
(pk, sk) ← Kgen
m0, m1
c ← Enc(pk, mb)
↳ RANDOMIZED ALGO !!
c
c' ≠ c
m'
b'
m' = Dec(sk, c')

Two constructions: Elgamal and RSA.

Elgamal:

*) PUBLIC PARAMETERS: (G, g, q)

*) KEY GEN: $pk = h = g^x$

$sk = x \; ; \; x \leftarrow \mathbb{Z}_q$.

*) ENC: Pick $r \leftarrow \mathbb{Z}_q$

$$C = (c_1, c_2) = (g^r, h^r \cdot m)$$

MESSAGE $m \in G$.

*) DEC: $c_2 / c_1^x = \frac{h^r \cdot m}{g^{rx}}$

$$= \frac{h^r \cdot m}{(g^x)^r} = \frac{h^r \cdot m}{h^r} = m$$

THM The above PKE is CPA-secure under DDH.

Proof. Start with $G(\lambda, b)$ the

CPA game and define $H(\lambda, b)$ where h^r is replaced by g^z for $z \leftarrow \mathbb{Z}_q$.

Now: $G(\lambda, b) \approx_c H(\lambda, b) \quad \forall b$.

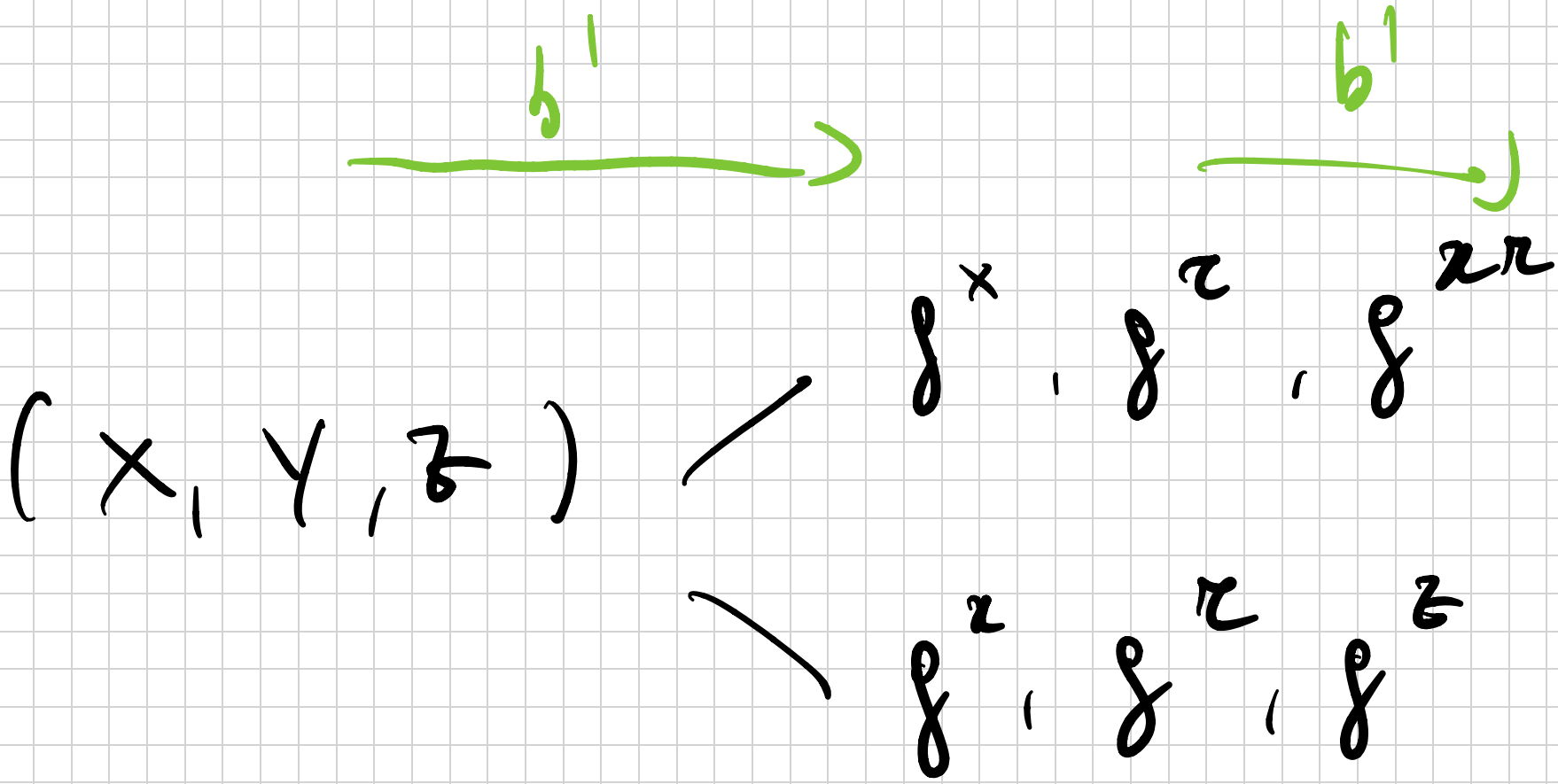
A_{CPA} $\quad$ A_{DDH} $\quad$ C_{DDH}

$pk = X$

X, Y, Z

m_0, m_1

$(Y, Z \cdot m_b)$



In first case the reduction symmetries $G(\lambda, b)$, in the second $H(\lambda, b)$

On the other hand : $H(\lambda, 0) \equiv H(\lambda, 1)$. ∎