REVISITING MINICRYPT

Recall: We have introduced hard problems

FACTORING, DL, CDH, DDH

Trivial: FACTORING, DL $\Rightarrow$ OWF

PRG?

$params = (\mathbb{G}, g, q) \leftarrow\$ Gen(1^n)$

SEED $\rightarrow x, y \leftarrow\$ \mathbb{Z}_q$

$PRG_{g,q}(x, y) = (g^x, g^y, g^{xy})$

$\mathbb{Z}_q^2 \rightarrow \mathbb{G}^3$

DDH $\Rightarrow$ PRG

DDH $\Leftrightarrow \approx_c (g^x, g^y, g^z)$

UNIFORM over $\mathbb{G}^3$

Better stretch: $Z^{t+1} \to G^{2t+1}$

$$PRG_{g,q}(x, y_1, \ldots, y_t) = (g^x, g^{y_1}, g^{xy_1}, \ldots, g^{y_t}, g^{xy_t})$$

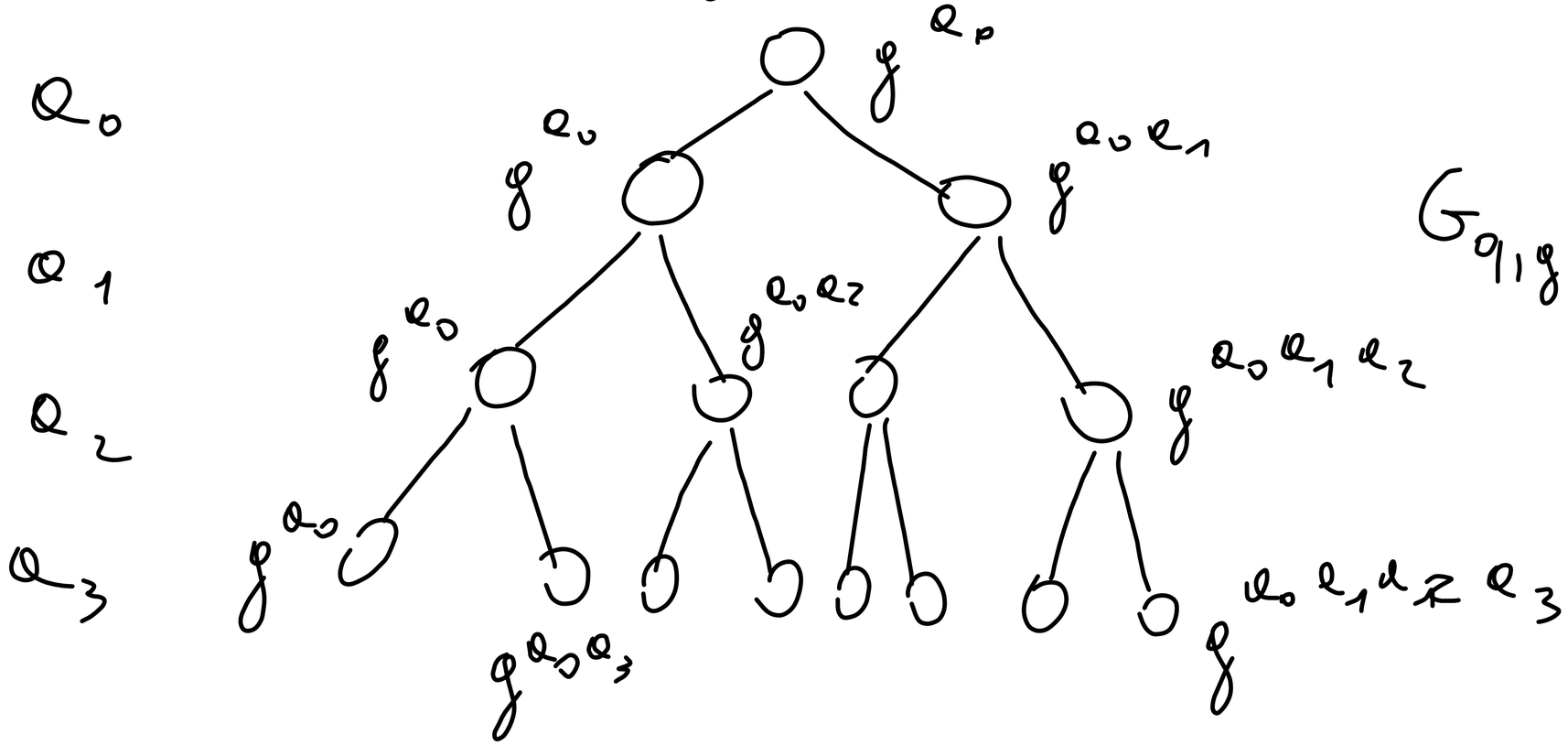
LEMMA. The above is also a PRG under DDH.

The proof consists of a hybrid argument.

DDH ⇒ PRF

$$F_{g,\vec{e}}(\underbrace{x_1,\dots,x_n}_{\in\{0,1\}^n}) = \left(g^{e_0}\right)^{\prod_{i=1}^{n} e_i^{x_i}}$$

$$\vec{e} = (e_0, e_1, \dots, e_n) \in \mathbb{Z}_q^{n+1}$$



$$G_{g,\vec{e}}(g^b) = (g^b, g^{eb})$$

$$= (G_0(g^b), G_1(g^b))$$

DL $\Rightarrow$ CRH :

$$H_{p,g_1,g_2}(x_1,x_2) = g_1^{x_1} \cdot g_2^{x_2} \mod p$$

$$\mathbb{Z}_q^2 \to \mathbb{G} = QR|R_p$$

$\exists$ PPT A : x_1, x_2, x_1', x_2' s.t. $(x_1,x_2) \neq (x_1', x_2')$

$$g_1^{x_1} g_2^{x_2} = g_1^{x_1'} g_2^{x_2'} \mod p$$

x_1, x_2

$g_1^{x_1} \cdot g_2^{x_2} = g_1^{x_1 + \alpha x_2}$

x_1', x_2'

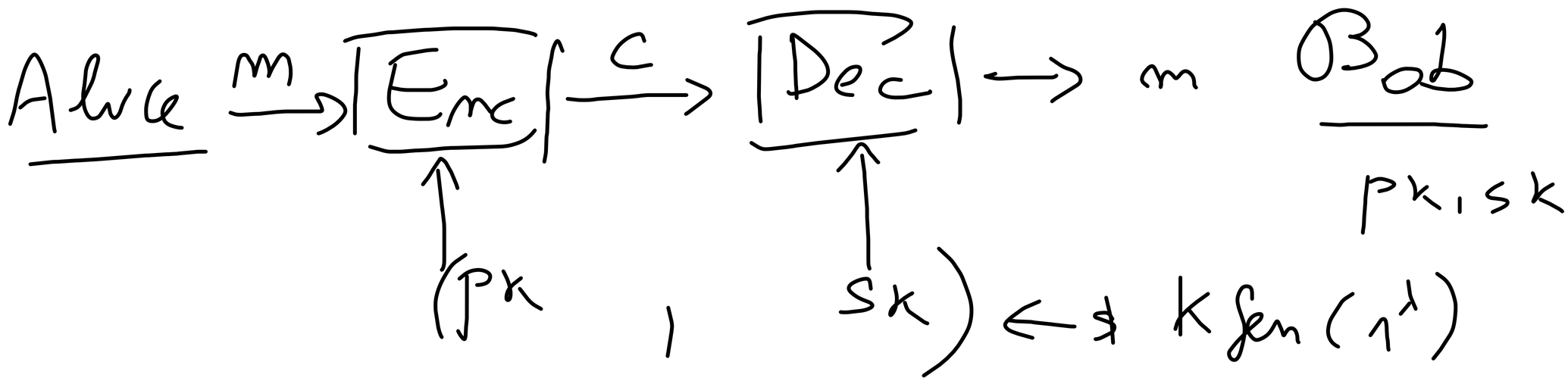
$x_1' + \alpha x_2' = x_1 + \alpha x_2$

$g_2 = g_1^{\bar{x}}$

$g_1^{x_1 - x_1'} = g_2^{x_2' - x_2} \mod p$

$g^{x} = g_1 = g_2^{(x_2' - x_2)\cdot(x_1 - x_1')^{-1}}$

PUBLIC-KEY ENCRYPTION



CORRECTNESS : $\forall \lambda \in \mathbb{N}, \forall m \in \mathcal{M}, \forall (pk, sk)$ by $Kgen(1^\lambda)$

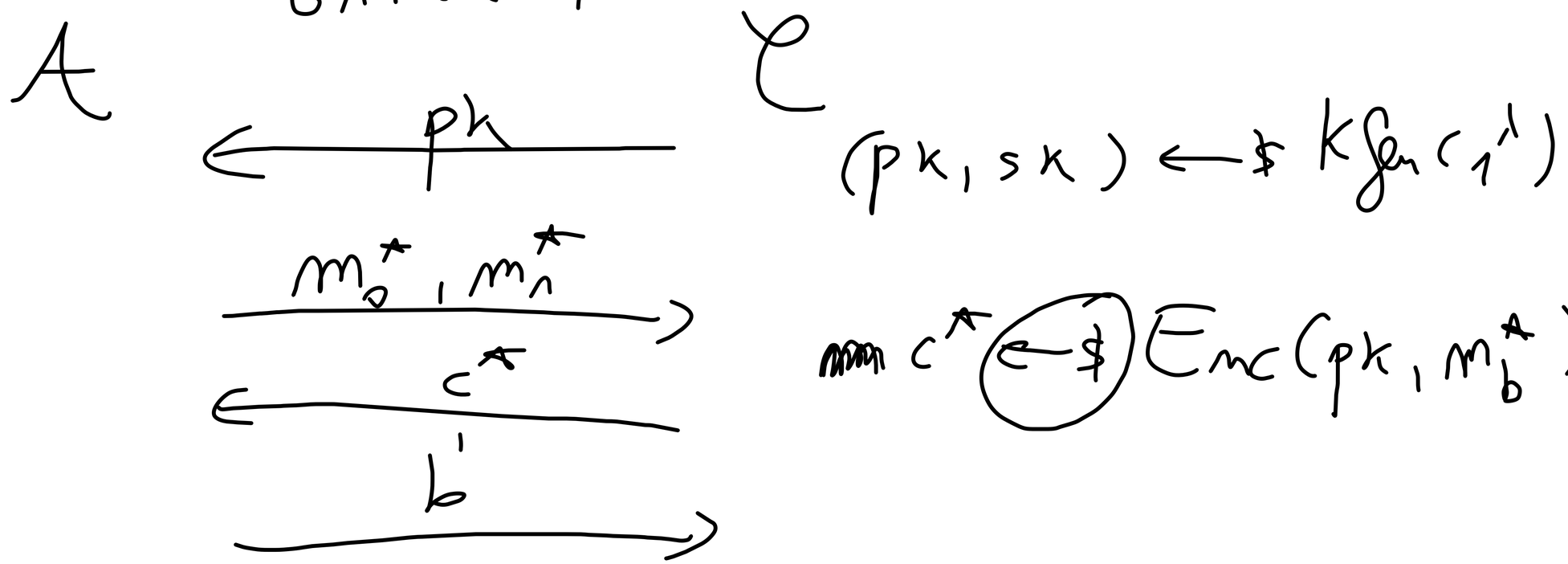
$$Dec(sk, Enc(pk, m)) = m$$ ✓

For later: Authenticity of PKs ?!?

DEF $\Pi = (KGen, Enc, Dec)$ is CPA-secure

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

$GAME(\lambda, b)$



How to get PKE?

RSA: 1978. FACTORING (?). $\mathcal{M} = \mathbb{Z}_n^*$

- $pk = (n, e)$; $sk = (n, d)$

$n = p \cdot q$; $e \cdot d \equiv 1 \bmod \varphi(n)$ ← $(p-1)(q-1)$

- $Enc(pk, m) = m^e \bmod n = c$

NOT CPA SECURE

- $Dec(sk, c) = c^d \bmod n = (m^e)^d \bmod n$

$= m^{e \cdot d} \bmod n = m^{t \cdot \varphi(n) + 1} \bmod n \equiv 1 \cdot m \bmod n$

$m^{\varphi(n)} \equiv 1$ by EULER $\equiv m$

How to fix it? PKCS #1.5

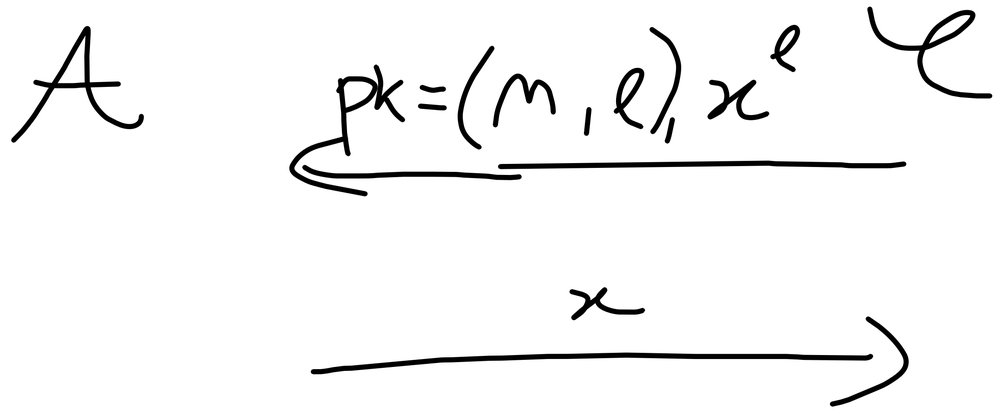
$$\hat{m} = r \| m \qquad r \xleftarrow{\$} \{0,1\}^{\ell}$$

$$c = \hat{m}^e \bmod n.$$

Is it secure? Under which assumption?

- For $r \in O(\log \lambda)$ NO. Because A can guess r
- For $r = \omega(\log \lambda)$? Nobody knows!
- For $m \in \{0,1\} \Rightarrow$ CPA secure: FACTORING? Don't know!

DEF (RSA). RSA assumption:



In other words: $f_{pk}(x) = x^e \bmod n$ es a OWF

RSA $\Rightarrow$ FACTORING

FACTORING $\Rightarrow$ RSA ?????