$$\mathbb{Z}_q^{\ell+1} \longrightarrow G^{2\ell+1}$$

Exercise: Prove this is secure from DDH.

*) PRFs. There is a simple construction of PRFs from DDH.

$$\mathcal{F}_{NR} = \{ F_{q,g,\vec{a}} : \{0,1\}^n \to G \}_{\vec{a} \in \mathbb{Z}_q^{n+1}}$$

$$\vec{a} = (a_0, a_1, \ldots, a_n)$$

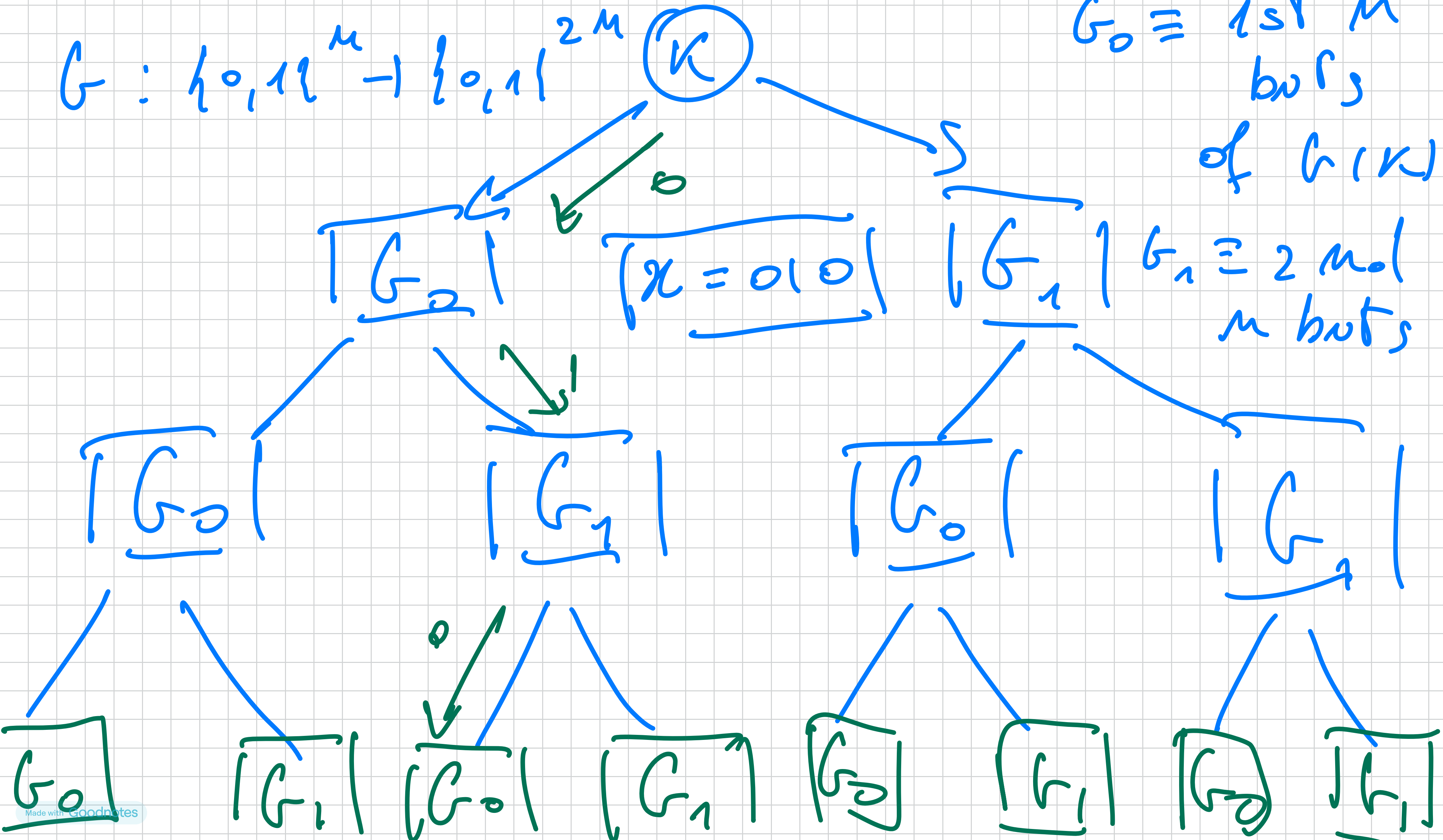
$$F_{q,g,\vec{a}}(x_1, \ldots, x_n) = \left(g^{a_0}\right)^{\prod_{i=1}^{n} a_i^{x_i}}$$

The security follows the same ideas of the proof PRGs $\Rightarrow$ PRFs (GGM).

$G : \{0,1\}^n \to \{0,1\}^{2n}$

$G_0 \equiv$ 1st n bits of $G(K)$

$G_1 \equiv$ 2nd n bits

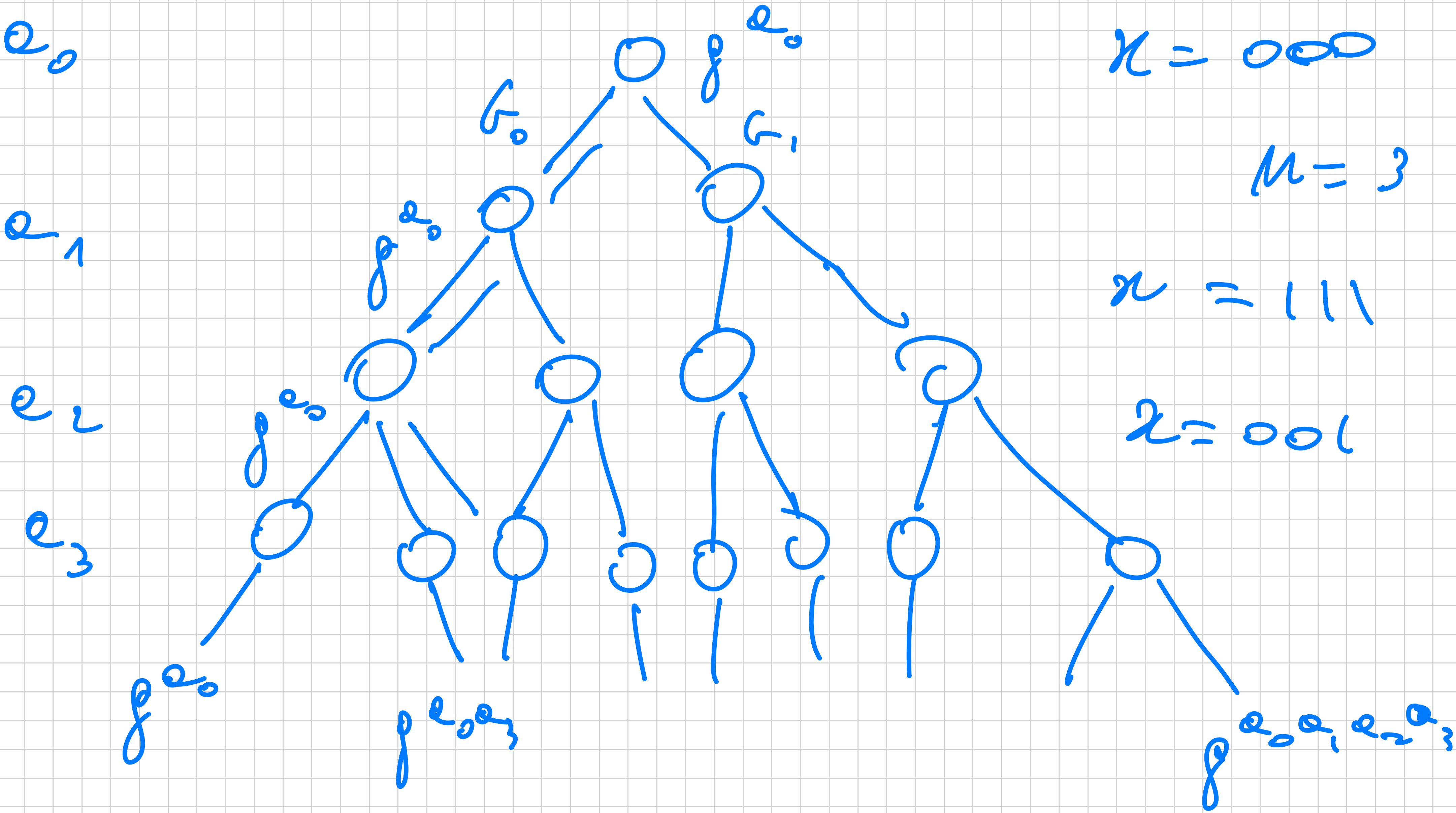


$F_k(x)$ where $x = x_1 \dots x_n$

Thm. If G is a PRG, GGM gives a PRF.

We can interpret the NR PRF as GGM with the following PRG:

$$G_{q,g,a}(g^b) = G_0(g^b) \| G_1(g^b)$$
$$= (g^b, g^{ab})$$



$x = 000$

$n = 3$

$x = 111$

$x = 001$

PUBLIC-KEY ENCRYPTION

$$
\begin{tikzcd}
\text{Alice} \arrow[r, "m"] & \boxed{\text{Enc}} \arrow[r, "c"] & \boxed{\text{Dec}} \arrow[r, "m"] & \text{Bob} \\
pk \arrow[ur] & \boxed{\text{KGen}} \arrow[rr] & & pk, sk \arrow[ul]
\end{tikzcd}
$$

CORRECT:

$$\forall m : \Pr[\mathrm{Dec}(sk, \mathrm{Enc}(pk, m)) = m] = 1$$

$\forall pk, sk$ (HONESTLY GENERATED)

DEF (CPA - SECURITY) $\Pi = (\mathrm{KGen}, \mathrm{Enc}, \mathrm{Dec})$

$\leadsto$ CPA-secure PKE if:

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

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

$\mathcal{A}$ $\qquad\qquad\qquad\qquad$ $\mathcal{C}$

$$\xleftarrow{\quad pk \quad}$$

$(pk, sk) \leftarrow \mathrm{KGen}(1^\lambda)$

$$\xrightarrow{\quad (m_0^*, m_1^*) \in \mathcal{M} \quad}$$

$c^* \leftarrow \mathrm{Enc}(pk, m_b)$

$$\xleftarrow{\quad c^* \quad}$$

$$\xrightarrow{\quad b' \quad}$$

$$\left| \Pr[\, b' = 1 : \mathrm{GAME}(\lambda, 0)\,] - \Pr[\, b' = 1 : \mathrm{GAME}(\lambda, 1)\,] \right| \leq \mathrm{negl}$$

The simplest PKE: ElGamal (1984).

$$(\mathbb{G}, g, q) \leftarrow \mathrm{GroupGen}(1^\lambda)$$

<u>$\mathrm{KGen}(1^\lambda)$</u> : $x \leftarrow \mathbb{Z}_q$; $h = g^x$

$sk = x$; $pk = h$.

$\underline{\mathrm{Enc}(pk, m \in \mathbb{G})}$: $c = (c_1, c_2)$

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

$r \leftarrow \mathbb{Z}_q$

$\underline{\mathrm{Dec}(sk, (c_1, c_2))}$: Output c_2 / c_1^x

Why does it work:

$$c_2 / c_1^x = \frac{h^r \cdot m}{(g^r)^x} = \frac{\cancel{h^r} \cdot m}{\cancel{(g^x)^r}}$$

THM ElGamal PKE is CPA secure under the DDH assumption in $\mathbb{G}$.

Proof. The idea is simple. By the DDH assumption

$$(g^x, g^r, \underbrace{g^{xr}}_{h^r}) \approx_c (g^x, g^r, g^z)$$

$z, r, x \leftarrow \mathbb{Z}_q$.

$\overline{|G(\lambda, b)|}$

$\mathcal{A}$		$\mathcal{C}$
$H(\lambda, b)$	$\xleftarrow{\ pk = h = g^x\ }$	$z \leftarrow \mathbb{Z}_q$
	$\xrightarrow{\ (m_0, m_1)\ }$	$c_1 = g^r$; $r \leftarrow \mathbb{Z}_q$, x
	$\xleftarrow{\ (c_1, c_2)\ }$	$c_2 = h^r \cdot m_b$
	$\xrightarrow{\ b'\ }$	$c_2 = g^z \cdot m_b$

Need to show: $G(\lambda, 0) \approx_c G(\lambda, 1)$.

1) $H(\lambda, 0) \equiv H(\lambda, 1)$ because c_2 is uniform over $\mathbb{G}$ and thus independent of b.

2) $H(\lambda, b) \approx_c G(\lambda, b) \quad \forall\, b \in \{0, 1\}$.

1) + 2) $\Longrightarrow$ THM

) Reduction to DDH

$$\mathcal{A} \xleftarrow{\;pk = X\;} \mathcal{B} \xleftarrow{\;(X, Y, Z)\;} \mathcal{C}_{DDH}$$

$X = g^{x}$

$Y = g^{y}$

$$\xrightarrow{m_0,\, m_1}$$

$$\xleftarrow{(c_1 = Y,\; c_2 = Z \cdot m_b)}$$

$$\xrightarrow{b'} \qquad \xrightarrow{b'}$$

Z — g^{xy}, g^{z}

$x, y, z \leftarrow \mathbb{Z}_q$

Perfect simulation:

$$c_2 = Z \cdot m_b \;\Big\langle\; \begin{array}{l} g^{xy} \cdot m_b = (pk)^y \cdot m_b \\ g^{z} \cdot m_b \text{ es un } G(\lambda, b) \end{array}$$

es un $G(\lambda, b)$

$\Pr[\mathcal{B} \text{ outputs } b' = 1] = \Pr[A \text{ outputs } b' = 1]$

$= \Pr[G(\lambda, b) = 1]$

↪ when X, Y, Z is a DDH Tuple

$\boxtimes$