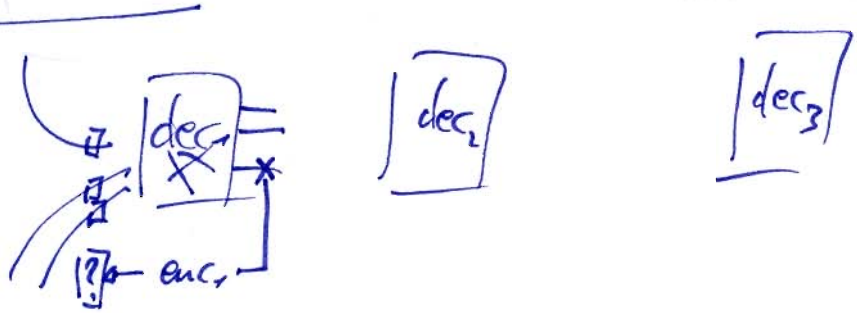
$enc_1(enc_2(enc_3(text)))$



$$enc_i = \begin{cases} RSA(text \,||\, rnd_i) \\ ElGamal_{rnd_i}(text) \end{cases}$$

$$ElGamal: (1, x) \longmapsto (g^\tau, a^\tau x)$$

$(1, x) = (g^0, a^0 x)$

decryption

reencryption

$$(g^\delta, a^\delta x) \longmapsto (g^\tau, a^\tau x)$$

$\tau = \delta$ + shuffle

$$x \xrightarrow{enc} (g^\tau, (a_1 \cdot \ldots \cdot a_s)^\tau x)$$

$$a_i := g^{\alpha_i}, \quad \Pi a_i = g^{(\Sigma \alpha_i)}$$

$\downarrow dec_1$

$$(g^\tau, (a_2 \cdot \ldots \cdot a_s)^\tau x)$$

$$x \longmapsto (g^\tau, a_s^\tau x) \longmapsto (g^{(\tau)}, \boxed{\tau_1}, a_{s-1}^{\tau_2} a_s^\tau x)$$

x ↓ enc

added help. secret randomness

$\tau = \sigma + \rho$

$(g^{\sigma}, a^{\sigma} x) \xmapsto{\text{reenc}} (g^{\tau}, a^{\tau} x)$

$((g^{\tau}), (a^{\tau} x)) \xmapsto{\text{dec}}$ $(a^{\tau} x) / (g^{\tau})^{\alpha}$

where $a = g^{\alpha}$

$(a_1 \cdot \ldots \cdot a_s)^{\tau}$ (a = $a_1 \cdot \ldots \cdot a_s$)

$x \xmapsto{\text{enc}} (g^{\tau}, a_1^{\tau} \cdot \ldots \cdot a_s^{\tau} \cdot x)$ ← g, g^{τ}, g^{α}

↓ dec_1 ← $a_1 = g^{\alpha_1}$: $(g^{\tau})^{\alpha_1} = a_1^{\tau}$

$(g^{\tau}, a_2^{\tau} \cdot \ldots \cdot a_s^{\tau} x)$

$\prod a_i = g^{\sum \alpha_i}$

↓ dec_2

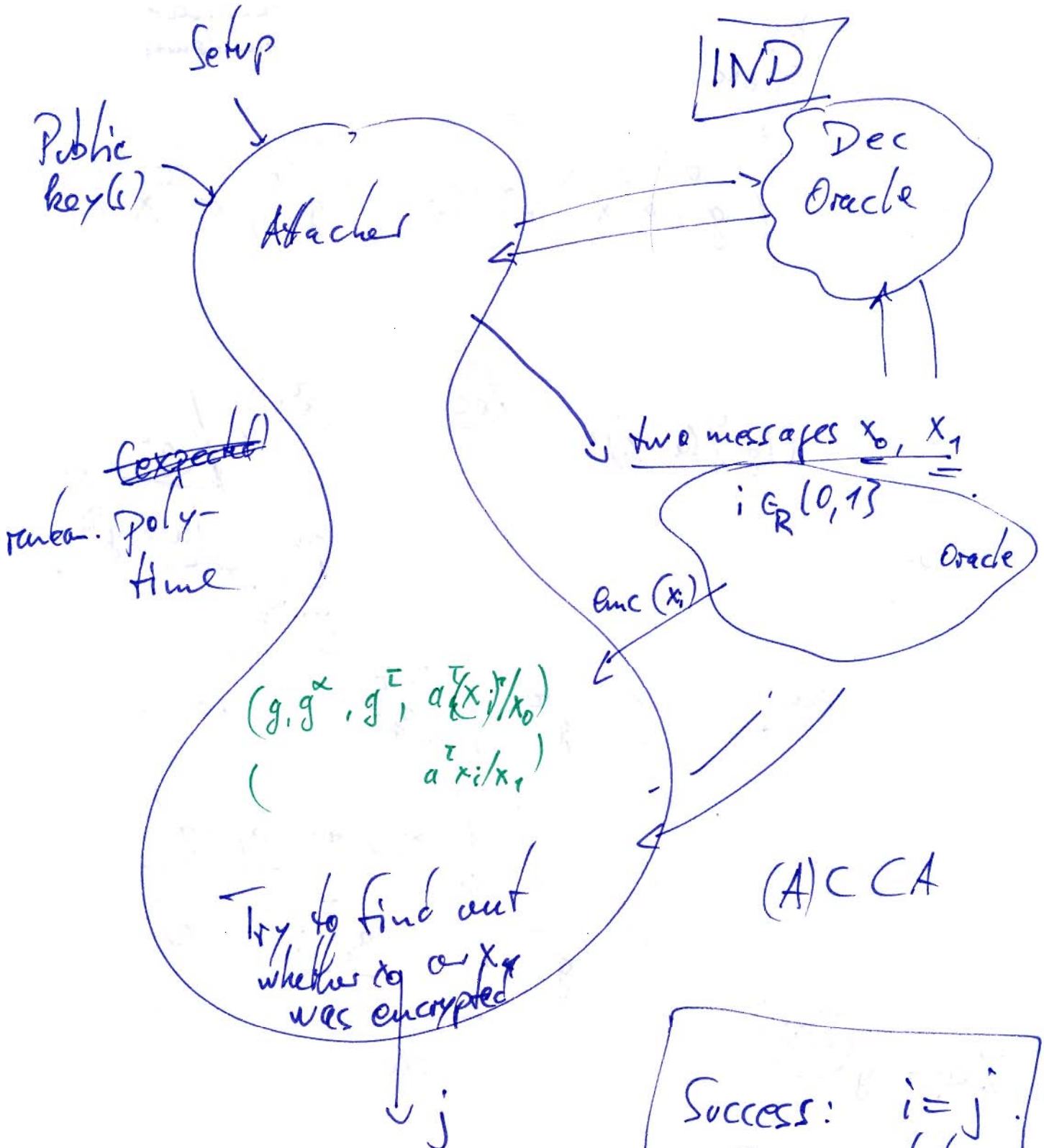
$(g, g^{\beta}, g^{\gamma}) \xmapsto{\text{DHP}} g^{\delta}$

$\delta = \beta\gamma$.

⋮

$a_s = g^{\alpha_s}$

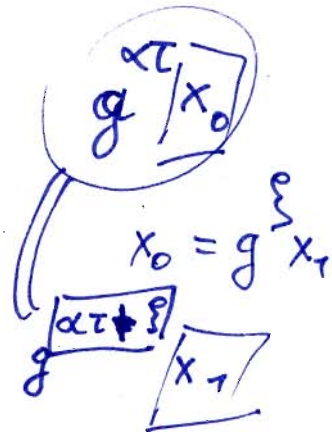
$(\not{x}, x)$


Setup
IND
Public key(s)
Attacker
Dec Oracle
two messages x_0, x_1
$i \in_R \{0,1\}$
Oracle
Enc (x_i)
$(g, g^\alpha, g^\tau, a^\tau x_i / x_0)$
$a^\tau x_i / x_1$
Try to find out whether x_0 or x_1 was encrypted
j
(A)CCA
Success: $i = j$
& never asked for decryption of x_0 or x_1 (or related)
$(g^\tau, a^\tau x_i)$
Security:
NO such attacker exist.
For example: reduce ElGamal-sec to DDHP

Reduces:

$(g, g^{\beta}, g^{\gamma}, g^{\delta})$

Q: $\delta = \beta\cdot\gamma$?



Take $a(=g^{\alpha}) = g^{\beta}$.

$t(=g^{\tau}) = g^{\gamma}$ $\quad a^{\tau} = g^{\alpha\tau}$

$y(=a^{\tau}x) = g^{\delta}\cdot x_i$

Good if case $\delta = \beta\gamma$.

Bad otherwise

Attacker tells us j for which he thinks that $y = a^{\tau}x_j$, $t = g^{\tau}$.

Case $\delta = \beta\gamma$: Attacker succeeds $\equiv$ we succeed. 100%

Output: Yes if $i = j$.

Case $\delta \neq \beta\gamma$ or easier to discuss: δ random.

→ Attackers answer is only a guess.

→ Output is correct = 50%.

NOT SECURE $\Leftrightarrow$ DDH solved.

$h = 2 \in \mathbb{Z}_p^\times$, $p = 12347$ ok

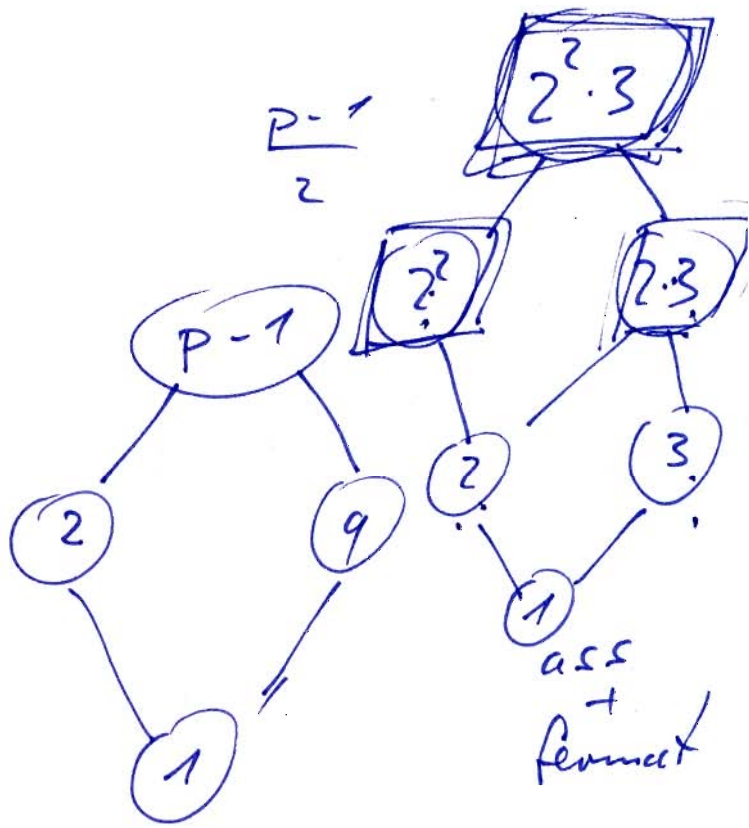
$q = \frac{p-1}{2} = 6173$.

$p - 1 = 2 \cdot q$.

$h^{p-1} \overset{\text{Fermat}}{=} 1$

$h^{\frac{p-1}{2}} = -1 \neq 1$

$h^{\frac{p-1}{q}} = 4 \neq 1$



Assume $h^\alpha = 1$

$0 < \alpha < p - 1$

Then $h^{\gcd(\alpha, p-1)} = h^{s \cdot \alpha + t \cdot (p-1)} = 1$,

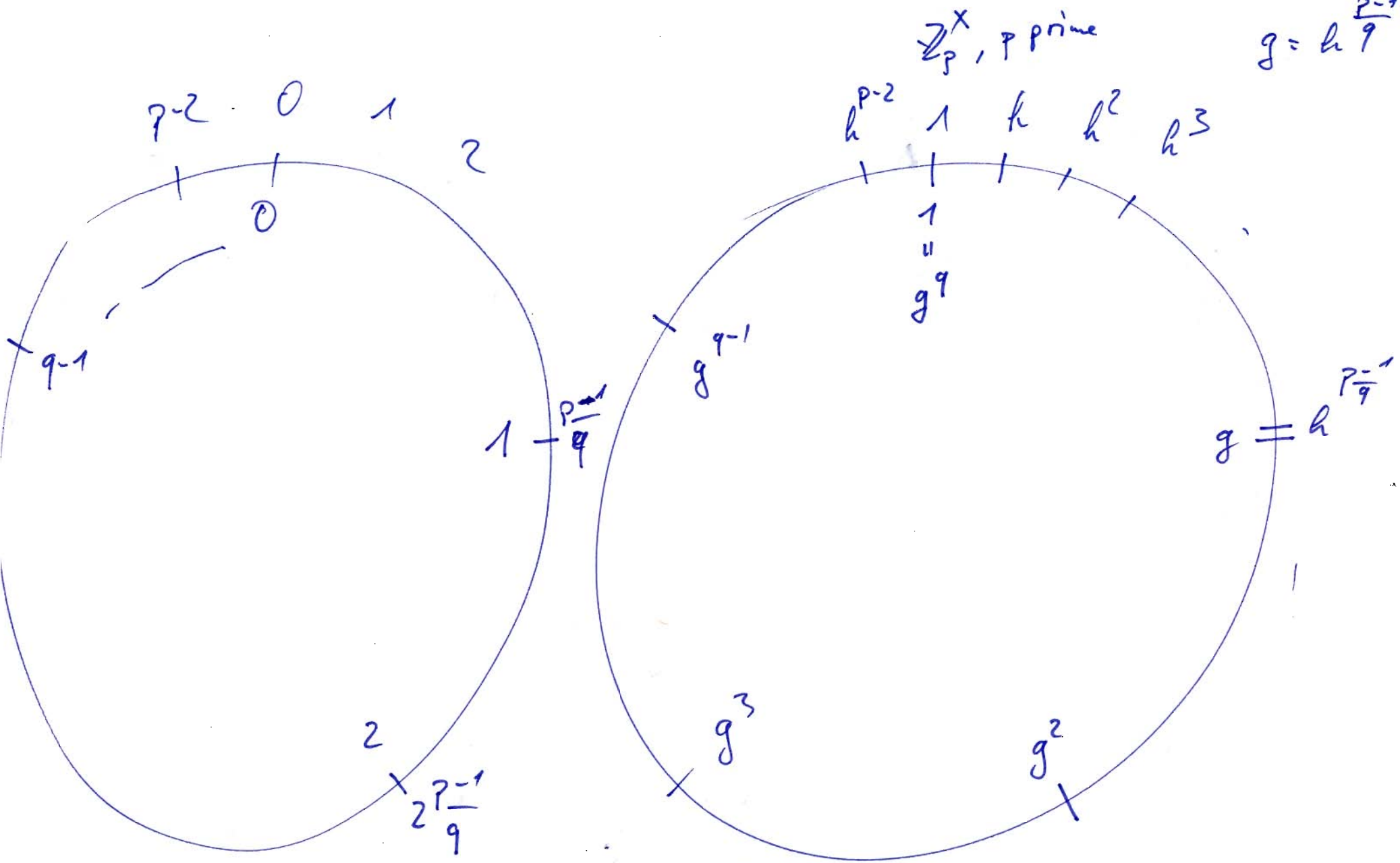
Wlog $\alpha \mid p-1$.

ie. $\alpha = 1$ or $\alpha = 2$ or $\alpha = q$ ... or $\alpha = p-1$

$\alpha = 2$: $\frac{p-1}{q}$

$\alpha = q$: $\frac{p-1}{2}$

$\frac{p-1}{\alpha}$ is prime.


$\mathbb{Z}_p^\times$, p prime
$g = h^{\frac{p-1}{q}}$
p-2
0
1
2
q-1
$1 - \frac{p-1}{q}$
$2\frac{p-1}{q}$
h^{p-2}
1
h
h^2
h^3
g^q
g^{q-1}
$g = h^{\frac{p-1}{q}}$
g^3
g^2