El Gamal

$\langle g \rangle = G$

ALICE

BOB

$\beta \in \mathbb{N}$ chiave privata

$b = g^\beta$ chiave pubblica

(b)

$m \in G$

k NONCE $\in \mathbb{N}$

$(x,y) = (g^k, b^k m) \longmapsto (x,y)$

$m = (x^\beta)^{-1} y$

Se si sa risolvere DLOG

- ricaviamo β da b
- ricaviamo k da $x = g^k$

$\downarrow$

$(b^k)^{-1} y = m$

1) ALICE può decodificare i propri messaggi.

2) El Gamal permette di codificare uno stesso messaggio in più modi differenti.

CAROL

$(x,y), m$

(x,y)

$(x',y) \neq (x,y)$ $\longrightarrow$ $m = m'$?

sono veramente indistinguibili codifiche differenti ($k \neq k'$) dello stesso messaggio?

Dipende anche da come sono rappresentati gli elementi del gruppo.

DISTINGUITORI (per un crittosistema) sono delle funzioni che consentono di individuare alcune proprietà specifiche del testo cifrato rispetto elementi casuali.

$(\alpha, \beta) \in G \times G$

CASUALE → (α_1, β_1) (α_2, β_2) ——— $(\alpha_{h+1}, \beta_{h+1})$

CODIFICHE DIFF. DEL MEDESIMO m → $(g^{i_1}, b^{i_1}m)$ $(g^{i_2}, b^{i_2}m)$ ——— $(g^{i_{h+1}}, b^{i_{h+1}}m)$

$o(b) \mid |g|$ con $o(b) < |G|$

3) El Gamal è omomorfico.

$(x_1, y_1) = (g^{k_1}, b^{k_1} m_1)$ $(g^{k_2}, b^{k_2} m_2) = (x_2, y_2)$

$\Rightarrow (x_1 x_2, y_1 y_2) = (g^{h+k}, b^{h+k} m_1 m_2)$ è una codifica di $m_1 m_2$

$(x_1, x_2) \longmapsto (x_1^{|G|}, x_2^{|G|}) = (1, 1)$

$(x_1, x_2) \longrightarrow (x_1^{|G|-1}, x_2^{|G|-1}) = (g^h, b^h m^{-1})$

Lemma: Sia G un gruppo finito, $x \in G$.

Allora $x^{|G|} = 1$ e dunque $x^{|G|-1} = x^{|G|} \cdot x^{-1} = x^{-1}$

DIM OSSERVIAMO CHE $|\langle x \rangle|$ ha ordine che divide $|G|$

$\Rightarrow x^{|G|} = x^{o(x)k} = 1^k = 1$ □

4) Re-encryption

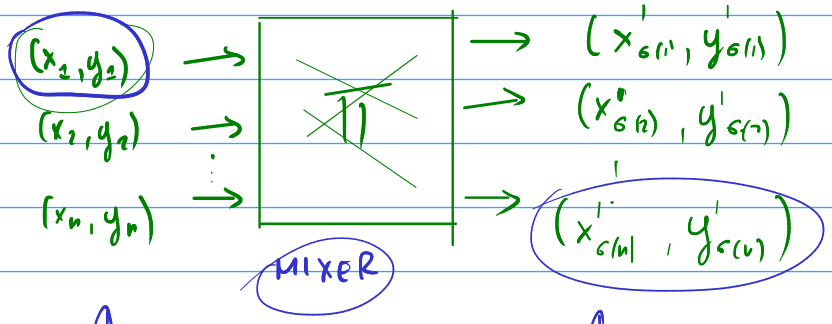
$(g^k, b^k m) = (x, y) \longrightarrow$ [Re-encr.] $\longrightarrow (x \cdot g^h, b^h \cdot y) =$

$= (g^{h+k}, b^{h+k} y)$

prende una codifica di m per BOB e ci fornisce una nuova codifica di m per BOB

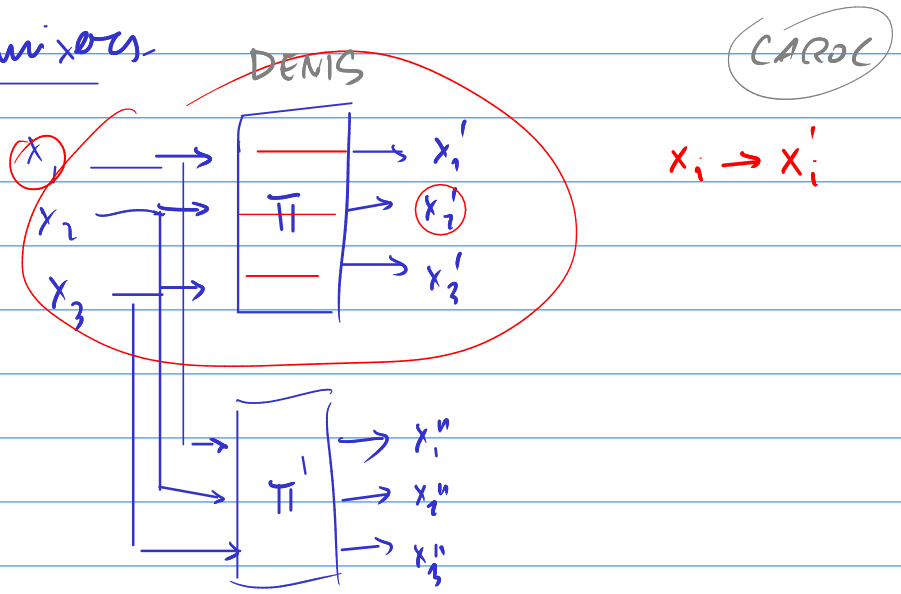
→ corrisponde a moltiplicare per una codifica del messaggio $m' = 1$ $(x', y') = (x, y) \cdot (g^h, b^h \cdot 1)$

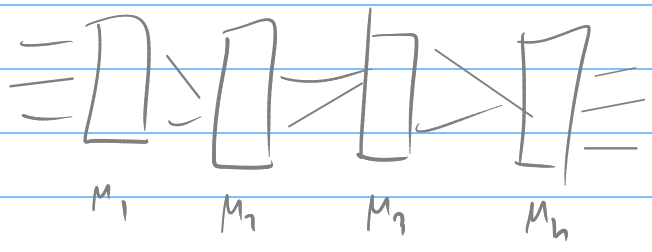
→ BASE DELLA NOZIONE DI MIXER CRITTOGRAFICO.



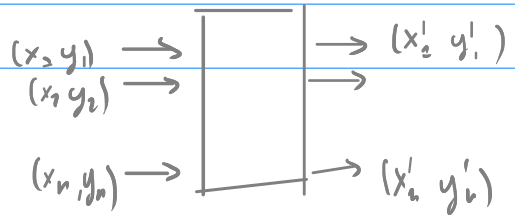
vogliamo garantire che l'input corrisponda all'output.

1) Shadow mixers.





per ElGamal una dimostrazione che i dati aggregati in input corrispondono ai dati aggregati in output senza rivelare le informazioni.



$(\alpha, \beta) = \Pi(x_i, y_i)$ $\quad \Pi(x_i', y_i') = (\alpha', \beta')$

sono entrambi codifiche del prodotto di tutti i messaggi m_i

$\left(g^{\sum k_i} \; b^{\sum k_i} \prod m_i\right)$ $\quad \left(g^{\sum (k_i + h_i)} \; b^{\sum (k_i + h_i)} \prod m_i\right)$

$(\alpha'', \beta'') = (\alpha', \beta') \cdot (\alpha^{-1} \; \beta^{-1}) = \left(g^{\sum k_i}, b^{\sum h_i}\right)$

in particolare $DLOG_g \alpha'' = DLOG_b \beta''$

DENIS DEVE DIMOSTRARE A CAROL CHE

DATI (α, β), (α', β') $\Rightarrow$ $DLOG_g \alpha' \alpha^{-1} = DLOG_b \beta' \beta^{-1}$

senza rivelare $\sum h_i$

→ WALLET DATA BASES WITH OBSERVERS

→ $G = \langle g \rangle$ $\quad h = g^x$

$m \in G$ $\quad z = m^x$

vogliamo dimostrare a CAROL che $\log_g h = \log_m z$

senza rivelare x

(prover) DENIS — (verifier) CAROL

$s = \text{NONCE}$

$(a, b) = (g^s, m^s)$

⟶ (a, b)

COMMITMENT

$c \in \mathbb{N}$ nonce

c ⟵

CHALLENGE

$r = s + cx$ ⟶ r

verifica

$$g^r = a h^c$$
$$m^r = b z^c$$

$$g^r = g^{\lambda + cx} = g^\lambda \cdot g^{cx} =$$

$$= g^\lambda h^c = a h^c$$

$$m^r = m^{\lambda + cx} = m^\lambda \cdot m^{cx} = b z^c$$

1) se i conti sono corretti la verifica va a buon fine.

2) effettivamente calcolare x

$\Rightarrow$ conoscere χ

$$(a, b) = (g^\lambda, m^\lambda)$$

$$c_1 \longrightarrow x_1$$

$$c_2 \longrightarrow x_2$$

$$g^{r_1} \quad g^{r_2} \quad m^{r_1} \quad m^{r_2}$$

$$g^{r_1 - r_2} = g^{(c_1 - c_2)x} = h^{c_1 - c_2}$$

$$m^{r_1 - r_2} = m^{(c_1 - c_2)x} = z^{c_1 - c_2}$$

$$\Rightarrow \log_g h = \frac{c_1 - c_2}{r_1 - r_2}$$

$$\log_m z = \frac{c_1 - c_2}{r_1 - r_2}$$

ops: avrei rivelato x

$$r_0 = s + cx \qquad \begin{cases} r_1 = s + c_1 x \\ r_2 = s + c_2 x \end{cases}$$

1) Se c'è un'unica challenge

CAROL ha una eq.

$r_0 = s + cx$ in 2 incognite (s ed x) e quindi non può determ. x (ci sono ∞^2 soluzioni).

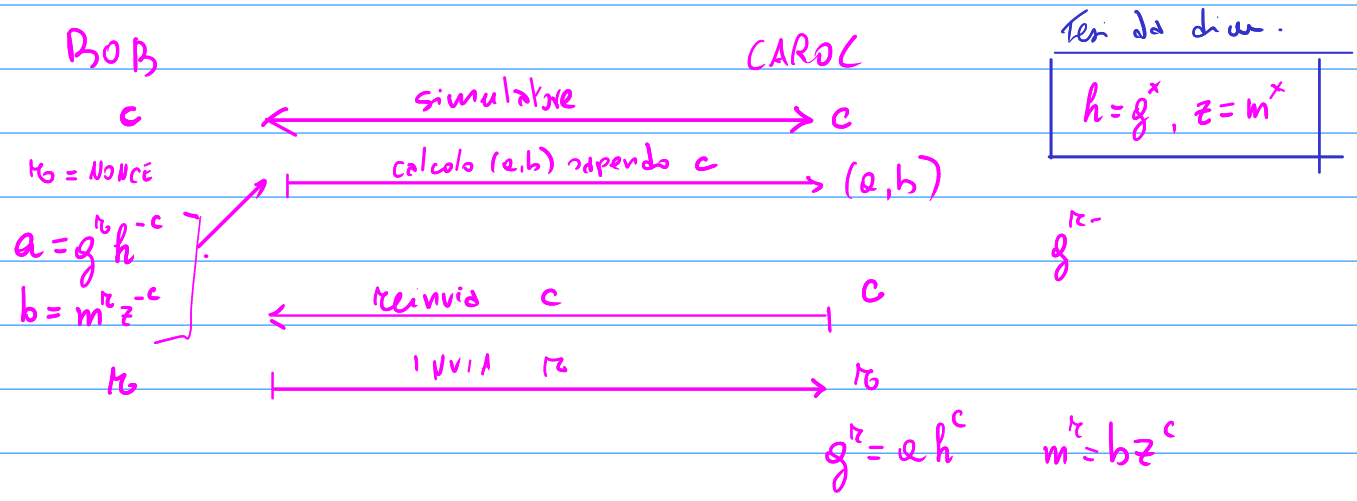
2) con 2 challenge distinte CAROL ha un sistema di 2 eq. indip in 2 incognite $\Rightarrow$ si calcola s ed x

---

PROTOCOLLO **ZKP** = Zero - Knowledge proof.

ZKP non è transitiva.

Verifica per il protocollo per DLOG.



SENZA CHE BOB CONOSCA x