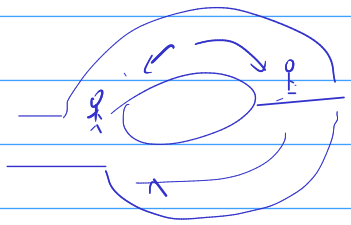
ZKP



OGNI PROBLEMA NP-completo ammette una dim. ZKP di soluzione.

P = esiste un alg. polinomiale per risolvere il problema

NP = esiste un algoritmo polinomiale per verificare una soluzione del problema.

$P \subseteq NP$ $\qquad$ $P \stackrel{?}{=} NP$

NP-completi

$x \quad g \quad m = g^x$ | NP

$m, g \quad DLOG_g(m)$

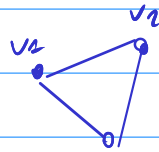
$p, q \longrightarrow n \stackrel{?}{=} pq$ | NP

DATO $n = p'q'$ trovare p', q'

3-colorazione di un grafo.

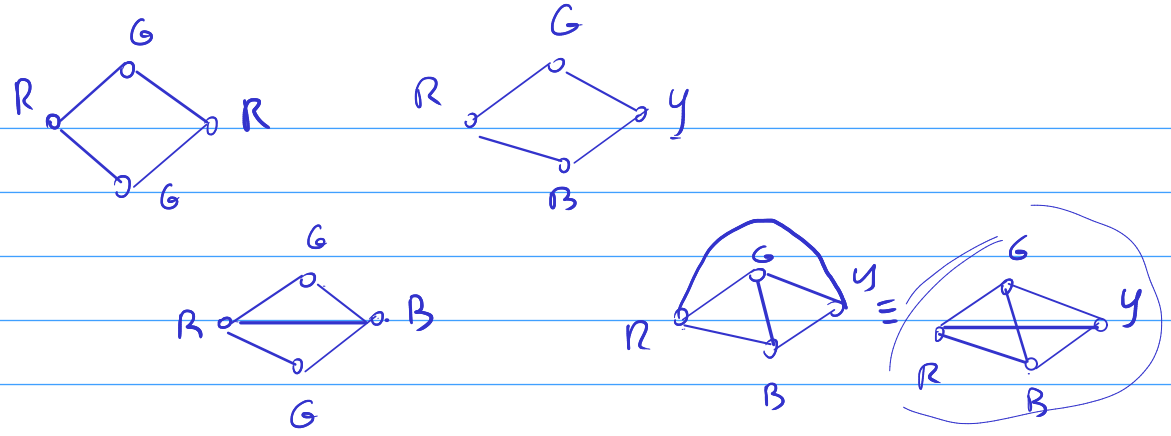
$\Gamma = (V, E)$ $\quad$ V insieme E insieme di sottoinsiemi di V di cardinalità 2

V vertici E spigoli



Dato Γ definiamo una colorazione $\chi: V \to \mathbb{N}$

come una funzione tale che $\forall v_1, v_2 \in V : \{v_1, v_2\} \in E \Rightarrow \chi(v_1) \neq \chi(v_2)$



p.b | dato Γ qual è il minimo numero di colori che si possono usare per colorarlo?

p.d dato Γ è possibile trovare una 3-colorazione di Γ?

↓

se avete una 3-colorazione ⇒ verificare che effettivamente sia giusta è facile.

$\forall e \in \mathcal{E}$ verificare $\chi(v_1) \neq \chi(v_2)$.

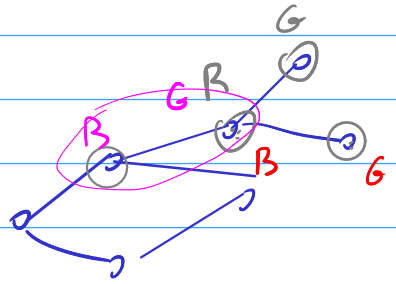
Trovarla è difficile → NP-completo

Denis	Carol
Ho una 3-colorazione di Γ.	
Γ grafo $\chi: \Gamma \to \{R,G,B\}$ colorazione.	$\Gamma = (V, \mathcal{E})$.
1) commitment. $\sigma \in S(\{R,G,B\})$.	
$\mathcal{C} = \{(v_i, \underbrace{\mathcal{E}_{k_i}(\sigma(\chi(v_i)))}_{l_i} \mid v_i \in V\}$	→ $\mathcal{C}$
(v_i, X_i)	2) challenge: sceglie v_i, v_j con $\{v_i, v_j\} \in \mathcal{E}$
←	

3) Risposde (proof)

(k_i, k_j) ⟶ (k_i, k_j)

4) Verify. $\quad \mathcal{D}_{k_i}(X_i) \neq \mathcal{D}_{k_j}(X_j)$



N.B La codifica dei colori non deve essere malleabile.

cioè dato $X_i = \mathcal{E}_{k_i}(\sigma(\chi(v_i)))$

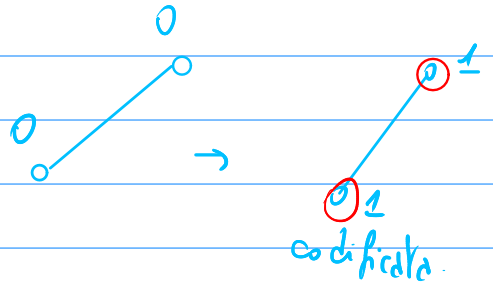
non deve esistere k_i' tale che

$\mathcal{D}_{k_i'}(X_i) \neq \sigma(\chi(v_i))$

$\mathbb{Z}_3 = \{0, 1, 2\}$ $\quad +1 \quad +2 \quad +0$

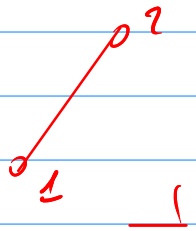
$\mathcal{E}_{k_1}(c_1) = 1$

$\mathcal{E}_{k_2}(c_1) = 2$



$k_1' = 1 \qquad k_2' = 2$

$\rightarrow \quad k_1' = 0, \quad k_2' = 1$



N.B ZKP si può usare anche per implementare schemi di autenticazione e/o firma digitale

El Gamal

ALICE

$G = \langle g \rangle$

$m \in G$

BOB

β chiave privata

$b = g^\beta$

b ⟵

k NONCE

(x, y) $(g^k, b^k m)$ ⟶ (x, y)

$m = x^{-\beta} y$

R: Come rappresentare i messaggi come elementi di G.

In realtà ALICE può anche usare un CRITTOSISTEMA SIMMETRICO

ALICE

m = messaggio

BOB

$(x, y) = (g^k, \mathcal{E}_{b^k}(m))$ ⟶ (x, y)

$m = \mathcal{D}_{x^\beta}(y)$

N.B. Questa variante non è più omomorfica in generale (→ non si può fare la re-encryption).

Firma digitale con DLOG $(\mathbb{Z}_p^*)$

FIRMA DIGITALE < NON RIPUDIABILE, NON FALSIFICABILE

per la non falsificabilità si pone uno schema di questo tipo.

$\sigma: M \times K_{priv} \longrightarrow S$ funzione che ad ogni messaggio ed ad ogni identità/chiave privata associa una firma

$v: M \times S \times K_{pub} \longrightarrow \{0,1\}$ funzione di verifica che dato un messaggio, una firma e una identità pubblica restituisce 0 oppure 1

$v\left(m, \sigma\left(m, k_{priv}^{ALICE}\right), k_{pub}^{ALICE}\right) = 1$

$v\left(m', \sigma\left(m, k_{priv}^{x}\right), k_{pub}^{ALICE}\right) = 0$ se $m' \neq m$ o $x \neq ALICE$

Siano (x_i, σ_i) una sequenza di messaggi x_i, con le relative firme σ_i

DICIAMO CHE LA FIRMA È ROBUSTA DAL PUNTO DI VISTA DELL'ESISTENZA SE

1) DATI $(x_1, \sigma_1), (x_2, \sigma_2) \dots (x_n, \sigma_n)$

EVE non riesce a far accettare una coppia (y', σ')

con $(y', \sigma') \notin \{(x_i, \sigma_i) \mid i = 1 \dots n\}$.

N.B Un cryptosistema simmetrico fornisce una forma di autenticazione

nel caso che la coppia $= (m, \underset{(x,y)=}{\mathcal{E}_k(m)})$ attesta che chi l'ha trasmessa conosce k (e quindi il destinatario accetta l'autenticazione $\iff \mathcal{D}_k(y) = x$ oppure $\mathcal{E}_k(x) = y$ (equiv.).

$\Rightarrow$ però ogni individuo in possesso di k può generare coppie valide).

AUTENTICAZIONE	FIRMA DIGITALE
CRITTOGRAFIA SIMMETRICA	CRITTOGRAFIA A CHIAVE PUBBLICA
segreto condiviso	funzione "a botola" chiave privata → chiave pubblica

DSA Digital Signature Algorithm

$\mathbb{Z}_p^*$

$\langle g \rangle$ sottogruppo ciclico $\cong \mathbb{Z}_q$ con q primo

$q \mid (p-1)$

BOB

x = chiave privata

$y = g^x \bmod p$

chiave pubblica

y, g

m = messaggio

$z = h(m)$

perché $g \in \mathbb{Z}_p^*$

k NONCE perché $ord(g) = q$

$r = (g^k \bmod p) \bmod q$

$s = (k^{-1}(z + x \cdot r)) \bmod q$

in $\mathbb{Z}_q$ quindi si calcola con l'alg. euclideo esteso

(r, s) ⟵ (r, s)

m

$z = h(m)$

$w = s^{-1} \bmod q$ → in $\mathbb{Z}_q$ (con l'alg. euclideo esteso)

$u_1 = (zw) \bmod q$

$u_2 = (rw) \bmod q$

verifica

$\left(\left(g^{u_1}\right)\left(y^{u_2}\right)\right) \bmod p\right) \bmod q = r$

$\left(\left(g^{u_1}\right)\left(y^{u_2}\right)\right) \bmod p$ → in $\mathbb{Z}_p^*$

$\bmod q$ → ? → razionale sull'ordine di g

$g^{u_1} = g^{(zw) \bmod q} \; g^{x(rw) \bmod q} = g^{w(xr+z) \bmod q}$

$= g^{s^{-1}(xr+z) \bmod q} = g^{k(xr+z)^{-1}(xr+z) \bmod q} =$

$= g^k \bmod p.$

MA $(g^k \bmod p) \bmod q = r$

$\Rightarrow \left(\left(g^{u_1} y^{u_2}\right) \bmod p\right) \bmod q = r$

N.B s^{-1} è calcolato modulo q perché g ha ordine q per costruzione $\Rightarrow g^q = 1$

$\Rightarrow s^{-1}$ è l'elemento $1 \le z \le q$ tale che $g^{zs} = g^{kq+1} = g$

RSA

Struttura di $\mathbb{Z}_n^*$ ove $n = p \cdot q$ con p, q primi.

$$\mathbb{Z}_n^* = \{ [a]_n \mid MCD(a, n) = 1 \}.$$

Supponiamo che $(\mathbb{Z}_n^*, \cdot)$ è un gruppo commutativo.

N.B se n non è primo $\Rightarrow \mathbb{Z}_n^*$ in generale non è ciclico.

$\varphi(n) = |\mathbb{Z}_n^*|$ quanto vale $\varphi(n)$?

$$MCD(a, n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \bmod n.$$

perché $[a] \in \mathbb{Z}_n^* \Rightarrow [a]^{|\mathbb{Z}_n^*|} = [1]$

$\Leftrightarrow a^{\varphi(n)} \equiv 1 \bmod n.$

p, q primi

$n = pq \Rightarrow \varphi(n) = ?$ $\quad n - \#\{\text{multipli di } p \text{ compresi fra } 1 \text{ e } pq\} - \#\{\text{multipli di } q \text{ compresi fra } 1 \text{ e } pq\} =$

$= n - q - (p-1) = n - p - q + 1 =$

$= (p-1)(q-1)$

N.B se conosciamo $p, q \Rightarrow$

$\varphi(pq) = (p-1)(q-1)$ FACILE DA CALCOLARE.

Se conosciamo $n = p'q'$ e $\varphi(n) \Rightarrow$ possiamo fattorizzare n.

$\varphi(n) = n - p' - q' + 1 \Rightarrow$

$\Rightarrow p' + q' = n - \varphi(n) + 1$

$(x-\alpha)(x-\beta) = x^2 - (\alpha+\beta)x + \alpha\beta$

$(x-p')(x-q') = x^2 - (p'+q')x + p'q' =$

$= x^2 - (n - \varphi(n) + 1)x + n$

Conoscere $(n, \varphi(n))$ ovvero (p, q) è equivalente.

Teorema cinese dei resti

Supponiamo di avere 2 congruenze

$$(*)\begin{cases} x \equiv \alpha_1 \mod \beta_1 \\ x \equiv \alpha_2 \mod \beta_2 \end{cases}$$

con $MCD(\beta_1, \beta_2) = 1$

$\Rightarrow \exists!\ \bar{x}$ con $0 \le \bar{x} < \beta_1 \beta_2$

che soddisfa $(*)$.

DIM

β_2 e β_1 sono coprimi.

$\Rightarrow \exists\ \overline{\beta_1}$ tale che $\overline{\beta_1} \cdot \beta_1 = 1 \mod \beta_2$

$\overline{\beta_2}$ tale che $\overline{\beta_2} \cdot \beta_2 = 1 \mod \beta_1$

poniamo $\bar{x} = \alpha_1 \overline{\beta_2} \beta_2 + \alpha_2 \overline{\beta_1} \beta_1$

$\bar{x} \mod \beta_1 = \alpha_1 \overline{\beta_2} \beta_2 \mod \beta_1 + \alpha_2 \overline{\beta_1} \beta_1 \mod \beta_1$

$= \alpha_1 \cdot 1 = \alpha_1$

$\bar{x} \mod \beta_2 = \alpha_2$ (similmente).

$\bar{x} + k(\beta_1 \beta_2) \equiv \bar{x} \mod \beta_1 \beta_2$

$$\begin{cases} \bar{x} = a_1 \mod \beta_1 = \bar{\bar{x}} \mod \beta_1 \\ \bar{x} = a_2 \mod \beta_2 = \bar{\bar{x}} \mod \beta_2 \end{cases}$$

con $0 \le \bar{x}, \bar{\bar{x}} < \beta_1 \beta_2 \qquad \bar{\bar{x}} \le \bar{x}$

consideriamo $\begin{cases} \bar{x} - \bar{\bar{x}} = 0 \mod \beta_1 \\ \bar{x} - \bar{\bar{x}} = 0 \mod \beta_2 \end{cases}$

$\beta_1 \beta_2 \mid (\bar{x} - \bar{\bar{x}})$

$\Rightarrow 0 \le \bar{x} - \bar{\bar{x}} \le \beta_2 \beta_1 - 1$

$\Rightarrow \bar{x} - \bar{\bar{x}} = 0 \Rightarrow \bar{x} = \bar{\bar{x}}$ □

$$\mathbb{Z}^*_{\alpha\beta} \cong \mathbb{Z}^*_\alpha \times \mathbb{Z}^*_\beta \qquad MCD(\alpha, \beta) = 1$$

Mostriamo innanzi tutto che

$(x, y) \in \mathbb{Z}^*_\alpha \times \mathbb{Z}^*_\beta$

$\Rightarrow CRT(x, y) = z \in \mathbb{Z}^*_{\alpha\beta}$ elemento ottenuto con th. cinese dei resti da (x, y)

$\exists\, \bar{x} \in \mathbb{Z}^*_\alpha, \ \bar{y} \in \mathbb{Z}^*_\beta$ tali che

$$\begin{cases} x\bar{x} = 1 \bmod \alpha \\ y\bar{y} = 1 \bmod \beta \end{cases}$$

$$z = \bar{\beta}\beta x + \bar{\alpha}\alpha y$$

$$\bar{z} = \bar{\beta}\beta\bar{x} + \bar{\alpha}\alpha\bar{y}$$

$$\begin{cases} z\bar{z} \bmod \alpha = x\bar{x} \bmod \alpha = 1 \\ z\bar{z} \bmod \beta = y\bar{y} \bmod \beta = 1 \end{cases}$$

in particolare $\begin{cases} z\bar{z} = 1 \bmod \alpha \\ z\bar{z} = 1 \bmod \beta \end{cases}$

$\Rightarrow$ per CRT ($\exists$ elemento $0 \le t < \alpha\beta$)

con $\begin{cases} t = 1 \bmod \alpha \\ t = 1 \bmod \beta \end{cases}$ e $t = 1$ va bene!

$\Rightarrow z\bar{z} = 1 \Rightarrow \bar{z} = z^{-1} \bmod \alpha\beta$

Viceversa: Supponiamo $z \in \mathbb{Z}^*_{\alpha\beta}$

$\Rightarrow \exists z^{-1}$ tale che $zz^{-1} = 1 \bmod \alpha\beta$

$\Rightarrow \begin{cases} zz^{-1} = 1 \bmod \alpha \\ zz^{-1} = 1 \bmod \beta \end{cases} \Rightarrow \begin{matrix} z \bmod \alpha \text{ invert.} \\ z \bmod \beta \text{ invertibile.} \end{matrix}$

$$|\mathbb{Z}_{\alpha\beta}^*| = |\mathbb{Z}_\alpha^* \times \mathbb{Z}_\beta^*| = |\mathbb{Z}_\alpha||\mathbb{Z}_\beta|$$

se $MCD(\alpha, \beta) = 1$

oss Se p primo $\Rightarrow |\mathbb{Z}_p^*| = p-1$

Se p^α potenza di primo

$$\Rightarrow |\mathbb{Z}_{p^\alpha}^*| = p^\alpha - p^{\alpha-1} =$$

$$= p^\alpha\left(1-\frac{1}{p}\right)$$

Se $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \Rightarrow$

$$\varphi(n) = |\mathbb{Z}_n^*| = p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right) p_2^{\alpha_2}\left(1-\frac{1}{p_2}\right) \cdots p_k^{\alpha_k}\left(1-\frac{1}{p_k}\right) =$$

$$= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

$n = pq$

$$n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right) = (p-1)(q-1)$$

□